Mako Networks Mako 7550-E

Product Handbook

v.1.1

Mako Networks Limited
Mako 7550-E Product Handbook
Version 1.1
©2008 Mako Networks Limited. All rights reserved.

The Mako logo is a registered trademark of Mako Networks Limited.
Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Information in this document is subject to change without notice and does not represent a commitment on the part of Mako Networks Limited.

No portion of this document may be reproduced in any form, or by any means, without prior written permission from Mako Networks Limited.

This document should be read in conjunction with the Mako Networks Limited Terms and Conditions available from the Mako Networks website (http://www.makonetworks.com).

Mako Networks, its parent or associate companies may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Mako Networks, its parent or associate companies, the furnishing of this document does not give you any rights or licence to these patents, trademarks, copyrights, or other intellectual property.

Table of Contents

Limited Warranty 4
Introduction 5
Unpacking and Connection 7
Turning on 9
MakoScope LCD 9
Login 10
Home 11
Reports: Usage 14
Reports: Status 26
Reports: Mako MailGuard 26
Reports: Licence Information 26
Configure 27
Configure: Internet 27
Configure: Network 31
Configure: Firewall 35
Configure: VPN 46
Configure: Services 55
Configure: Location 58
Configure: Access 59
Management: Home 60
Management: Company 60
Management: User 61
Help: Help Contacts 66
Help: Documentation 66
Help: Known Issues 67
Troubleshooting 68
Glossary of Terms 69

Limited Warranty

a) Standard Limited Warranty. If the products purchased hereunder are resold by a distributor or reseller to an end-user (customer) pursuant to the terms hereof in their original, unmodified, unused condition, Purchaser shall pass on to its customers, or keep as applicable for internal use, the MAKO NETWORKS, LTD. standard limited warranty for the products, as summarized in documentation supplied with the product and including provisions and limitations set forth below. The Manufacturer warrants the Mako appliance for one (1) year. The Warranty begins on the date of purchase as shown on your providers invoice.

b) Express End-user Limited Warranty. Each MAKO NETWORKS, LTD. product purchased hereunder is warranted against defect in material and workmanship and will substantially conform to MAKO NETWORKS, LTD. product documentation for the period set forth in the documentation supplied with the product following delivery to end-user (the “Warranty Period”). This warranty extends only to end-user and will not extend to, nor may it be assigned to, any subsequent user, Purchaser or user of a MAKO NETWORKS, LTD. product, whether such MAKO NETWORKS, LTD. product is alone or incorporated into end-user’s product.

c) Exclusions. The express warranty set forth above is contingent upon the proper use of a MAKO NETWORKS, LTD. product in the application for which it was intended and will not apply to any MAKO NETWORKS, LTD. product that has been (i) damaged during shipping, (ii) modified or improperly maintained or repaired by a party other than MAKO NETWORKS, LTD. or its designees, or (iii) subjected to unusual physical or electrical stress. This includes operation of the product outside the Operating Specifications of the product.

d) Limitation of Remedy. In the event a MAKO NETWORKS, LTD. product fails to perform as warranted, MAKO NETWORKS, LTD. sole and exclusive liability and end-user’s only remedies for breach of this warranty shall be, at MAKO NETWORKS, LTD.’s option to repair, replace or credit an amount not exceeding the Purchaser’s purchase price of each product found to be defective, provided that:

1. End-user complies with the rejection and warranty procedures contained in Section 5 below and returns the MAKO NETWORKS, LTD. product that the end-user considers defective for examination and testing.

2. MAKO NETWORKS, LTD. shall not be liable under this warranty if testing and examination by MAKO NETWORKS, LTD. discloses that the MAKO NETWORKS, LTD. product has been modified or altered in any manner after it was shipped by MAKO NETWORKS, LTD.

3. MAKO NETWORKS, LTD. shall not be liable under this warranty if testing and examination by MAKO NETWORKS, LTD. discloses that the alleged defect in the MAKO NETWORKS, LTD. product does not exist or was caused by end-user or any third person’s misuse, neglect, improper installation or testing, unauthorized attempts to repair or any other cause beyond the range of intended user, or by accident, fire or other hazard.

4. MAKO NETWORKS, LTD. shall not be liable under any warranty under this Agreement with respect to any MAKO NETWORKS, LTD. product that is not returned in its original shipping container or a functionally equivalent container.

5. If MAKO NETWORKS, LTD. testing and examination does not disclose a defect warranted under this Agreement: MAKO NETWORKS, LTD. shall so advise Purchaser and dispose of such MAKO NETWORKS, LTD. product in accordance with Purchaser’s instructions on behalf of end-user and at Purchaser’s cost.

Introduction

The Mako Networks System combines a web server driven configuration, management and reporting user interface with client end hardware to provide users with considerable cost savings as well as functionality and flexibility not currently available in traditional devices used to meet either the same or similar requirements. The Mako Networks System is targeted at small to medium sized businesses (SME), small to medium sized branch office of larger organisations and their use of broadband as a data transfer medium.

Mako 7550-E Firewall/Router/VPN Appliance
The Mako 7550-E by Mako Networks is a solid-state ethernet router with a stateful inspection firewall, VPN functionality and four LAN Ethernet ports. Designed to work in conjunction with the Mako Networks Central Management System, it provides you with enterprise level control over your connection to the Internet.

Complete Security
Your Mako 7550-E is managed by the Mako Networks Central Management System giving you complete peace of mind that your networks are always fully protected. All software is updated and patched automatically for you and intrusion attempts are dealt with. Your Mako 7550-E incorporates a stateful inspection firewall. This means that all traffic entering and leaving your networks is analysed comprehensively to ensure network integrity.

Firewall
Central to the security of your networks is the type of firewall you use. The Mako 7550-E utilises a stateful inspection firewall. A stateful inspection firewall does not just examine packets of information, instead it makes decisions based upon information derived from all communication layers and from other applications. This type of firewall provides true enterprise level protection. Working with the Mako Networks Central Management System, you have full control over all traffic entering and leaving your networks.

Four Networks
The Mako 7550-E protects up to four separate networks. This allows you to segregate your networks as you see fit.

Ethernet Router
An Ethernet Router is incorporated in to your Mako 7550-E connecting your networks to the Internet at high speed. You have the option to connect directly to an Ethernet connection to the Internet or via any other connection medium that supports Ethernet forwarding.

VPN
Virtual Private Networks allow you to assign secure remote access to your networks over the Internet. You can link two Mako protected networks together using the Mako Networks Central Management System in seconds with just three mouse-clicks! Linking three or more Mako protected networks is just as easy. The Mako Networks Central Management System allows this to happen without static IP addresses. In the same way you can also allow specified users remote access to your Mako protected networks with the Remote VPN feature. This is very useful for accessing your networks from home or while traveling.*

Logging/Reporting
Whilst all traffic from your Mako 7550-E goes directly out onto the Internet, your Mako sends traffic information securely to the Mako Networks Central Management System. This gives you the ability to monitor and control your Internet usage from anywhere in the world with Internet access. Simply log onto the Mako Networks website to view your usage, see how your broadband internet connection is being used, monitor where PCs on your network have been going and much more. And with MakoScope VGA feedback, you can easily see what your Mako is doing in real time.

---

* Third Party software may be required.

24 Hour Remote Control
Because your Mako utilises the Mako Networks Central Management System, you or your designated IT Professional have 24 hour secure remote control over your connection to the Internet. Via the Mako Networks website, you can modify firewall rules, create and disable VPNs, check usage patterns and even change your networks' IP addressing.

Automatic Updates
Because the Mako 7550-E is a centrally managed device, its software is kept up to date automatically. The Mako Networks Central Management System looks after all software updates, security patches and system updates for you. You can be assured that your Mako 7550-E will continue to be current as long as it has an up to date service licence.

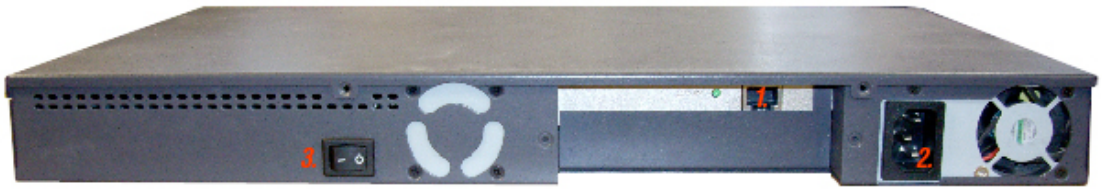
Optional Feature Enhancements
The Mako 7550-E gives you the option to incorporate optional feature enhancements such as Advanced Content Filtering, Email Sanitisation and Spam protection as well as virus protection. New features and options are being added all the time. Make sure you keep up to date by regularly logging into www.makonetworks.com.

Unpacking and Connection

Opening the carton you should find the following items:

- 1x Mako Device
- 1x Power Cord
- 2x Cat-5 Ethernet Cables
- Documentation CD
- Rack mounting kit
- USB Key – *may not be supplied depending upon your location*

What Goes Where
Place the Mako device in a convenient spot adjacent to your LAN hub(s) or switch(es) and the incoming Ethernet connection or Ethernet-Terminated Modem/NTU. For preference the location should be off the floor, out of direct sunlight and well ventilated, with a computer compatible power socket available.



Mako 7550-E Rear Panel

KEY
1. Ethernet WAN Port
2. Power Socket
3. Power Switch

Mako 7550-E Front Panel

KEY
1. LCD Screen
2. LCD Keypad
3. Diagnostic Port (authorised use only)
4. USB Ports
5. LAN 1 Port
6. LAN 2 Port
7. LAN 3 Port
8. LAN 4 Port

Connect cables to their corresponding sockets on the Mako. Connect the Power Cable to the mains supply. Connect the WAN Port to the network service providers termination point or an Ethernet-terminated Modem/NTU. Connect LAN Cables to your networks hub or switch.

DO NOT TURN YOUR MAKO ON AT THIS STAGE!

If this is the first time you are using your Mako, place the supplied USB Key in any USB port at the front of your Mako – *If your Mako was not supplied with a USB Key you do not need one in your location and can skip this step.*

What will be needed
There are a few special circumstances to be aware of:

HUB OR SWITCH PORT
Your office network needs to have an RJ-45 connection Port available for the Mako. If your network hardware does not have a spare 10/100 Ethernet Port available, you will need to either upgrade your existing hardware to increase the available Ports, or install an additional hub or switch.

DIRECT CONNECTION TO A COMPUTER
Normally the Mako is connected between the WAN port and a hub or switch device on your office network.

If you are connecting directly to a computer you will not need to obtain an Ethernet crossover cable or equivalent device. Your Mako 7550-E incorporates Auto Cross LAN Ethernet Ports.

POWER SUPPLY
The Mako has an adaptive power supply which sets itself to match the supply voltage provided at your site.

Connecting to your Internet service
Network Service Provider
Internet services are provided by a variety of network service providers in each country. In many cases the network service provider will be your local telephone supplier.

Network service providers have a variety of procedures for approving customer premises equipment for connection to their network. The connection interface in the Mako has been developed to connect to the majority of network service providers. If you have any queries your reseller will be happy to confirm whether the Mako is approved by your network service provider for connection to their telecommunications network.

Service Provider Manual
Your Network Provider can provide you with a Manual which covers all aspects of connecting to their Internet service. Please refer to this for any additional information you require.

Firewall and VPN Router Operation
Under normal conditions there is nothing which requires your intervention. The Mako is designed to detect many forms of internal malfunction and reset itself to correct operation.

In the worst case this may require it to download a fresh configuration from the Mako Networks' Central Command Servers. You can force a reload by a simple power off and on of the unit.

Changes to the configuration of the Mako cannot be made on the unit itself. These are performed by securely accessing and using the convenient menus on the Central Management web site https://secure.makonetworks.com.

Turning on

There are three lights on the front panel—only two, the Power light and the Status light are utilised at present.

When turning on for the first time the unit will connect directly to the Central Command Servers to download its configuration. The Power light should be on as download of the secure profile takes place.

Once your profile has been downloaded from the Central Command Servers, the Status light will illuminate green and your Internet communications are now established.

Please allow up to five minutes for the line light to illuminate green and your Mako to be ready for use.

MakoScope LCD

MakoScope LCD is the name for the Mako 7550 LCD Feedback System. By interacting with the LCD screen on the front of your Mako, you can get real time information of the status of your Mako.

MakoScope LCD

The MakoScope LCD shows the following useful information:

- Internet Status - If the Mako is online, your public IP Address is shown otherwise “Offline” will be displayed.
- WAN Interface Information - If connected, will display your media connection speed, otherwise will display “Down”.
- LAN Interface Listing - IP Addresses of your LAN interfaces.
- Mako ID – The unique identifier of your Mako

Testing
You can test whether you have Internet communications established by opening a web browser on one of your office computers and accessing two or three web sites. For example, a news web site (e.g. www.cnn.com) or a search engine (e.g. www.google.com).

If you are having difficulties do try more than one web site as they are sometimes “off the air” for various reasons of their own. If web browsing services work then Internet access is functional and all other services should be available.

Possible problems and their symptoms

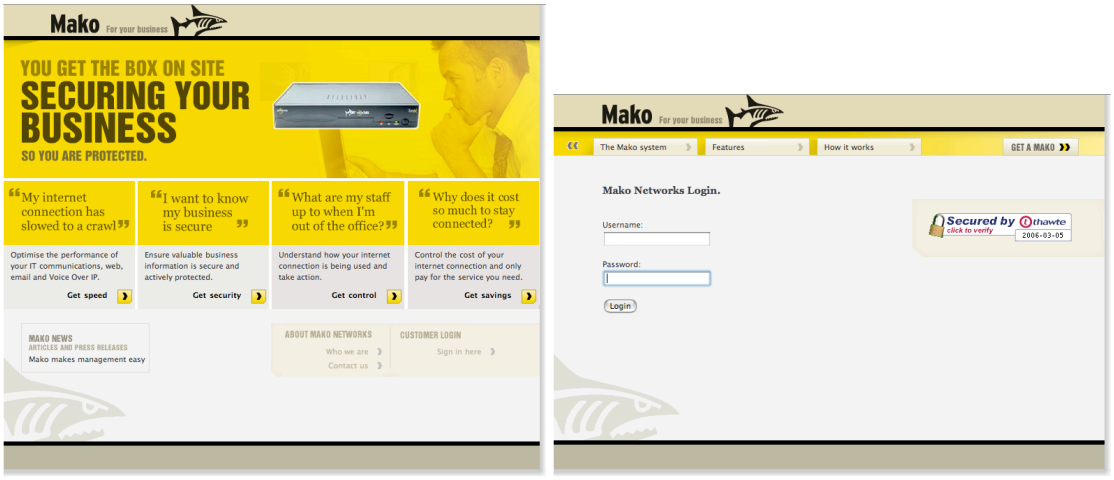
- A problem on the Internet circuit. If you believe that the line is at fault, please contact your Internet Service Provider Help Desk for status information on the circuit. They will work in conjunction with the network service provider to resolve the problem.

- A faulty profile, if the configuration profile of your unit has recently been changed. Another possibility is that the network Gateway configuration of your office computers has been changed. If you believe the problem is with the Mako then please contact your reseller, who will be able to check the status of the unit and verify the profile.

- Some computers on your office network can access the Internet, others cannot. Or perhaps some services work but others do not. Both of these indicate a faulty configuration of the network and/or computers in your office. If you believe the problem is with the configuration of the network and/or computers in your office, then please contact your site support organisation.

Login

Open your Web browser and type http://www.makonetworks.com into the Address or Location box, depending on your browser software. Click on Customer Login.



Mako Networks Home Page & Login Screens

Login
To administer your Mako appliance(s), enter your user name and password. Then click Login.

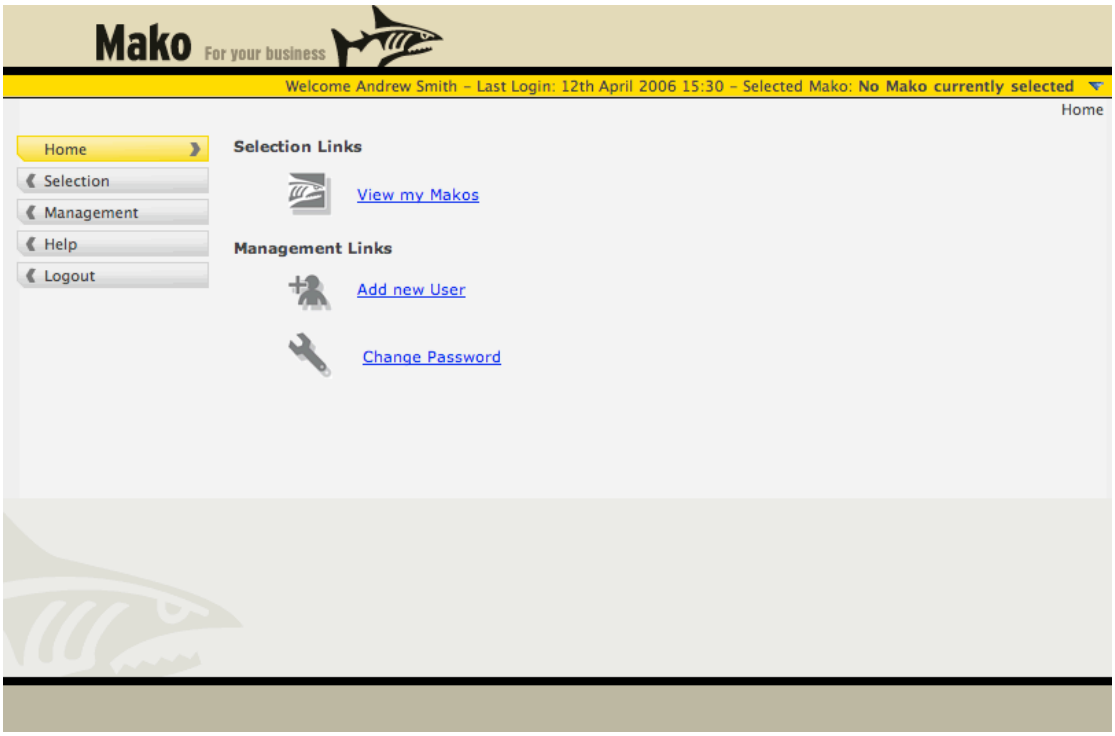
Remote VPN
To log in to the web site to start a remote secure IPSec VPN session, enter your user name and password, then click Login. The process is detailed in the Operations Guide section: VPN: Remote Access.

Considerations

- The Mako Networks web site has been tested against several versions of the popular browser software products. It is likely that different browser products, versions and settings will format screen displays slightly differently.
- Please note that you must accept Cookies to access the Mako Networks web site, and that you must have JavaScript enabled. These properties are set in your browser preferences.
- While accessing the Mako Networks web site your browser will be switched into a secure mode, known as SSL, in which traffic between the browser and the Central Command Servers is encrypted.

Home

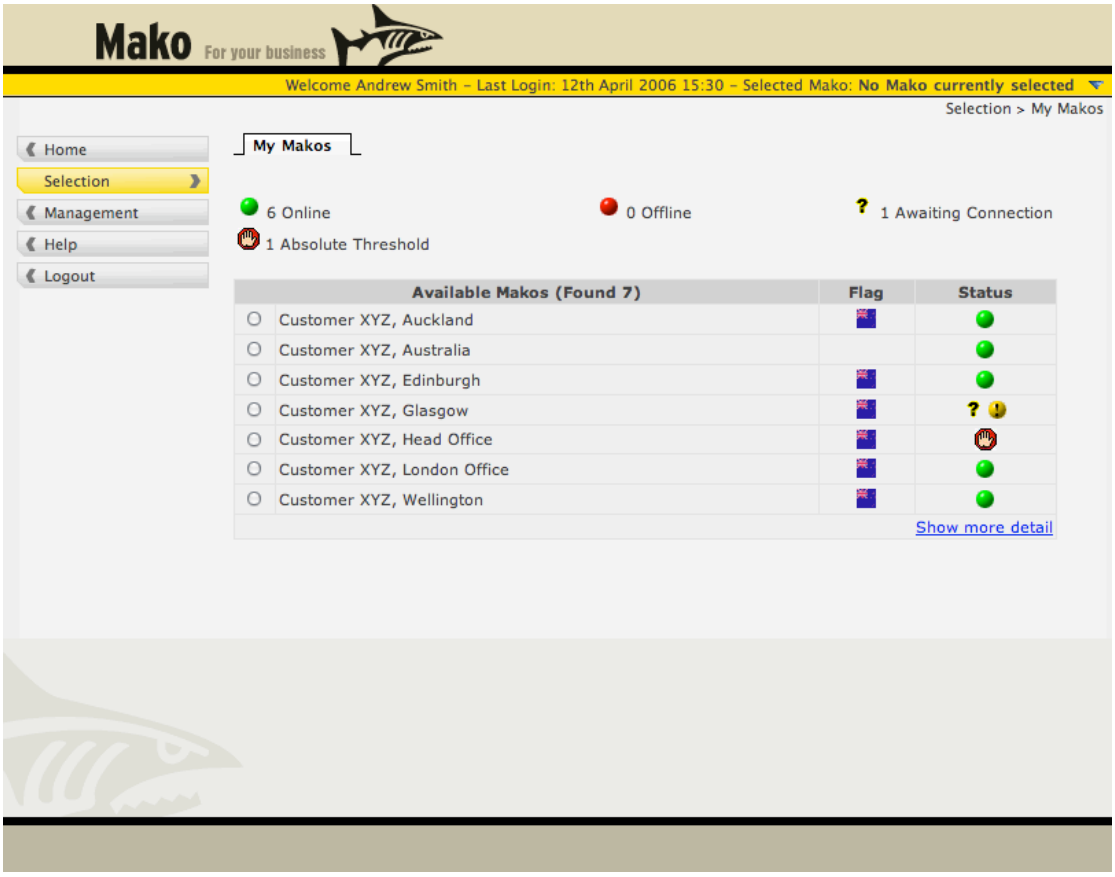
Once your Login is successful a screen like the one below will be displayed. This is the starting point for administration of your Mako devices and Users.



Home Screen

This document will cover Adding a New User in the Management section. For now, click on View my Makos or click on the Selection menu to go to the Selection screen.

Alternatively, you can click on Change Password to change the password for the account you used to log in to the Mako Networks site.



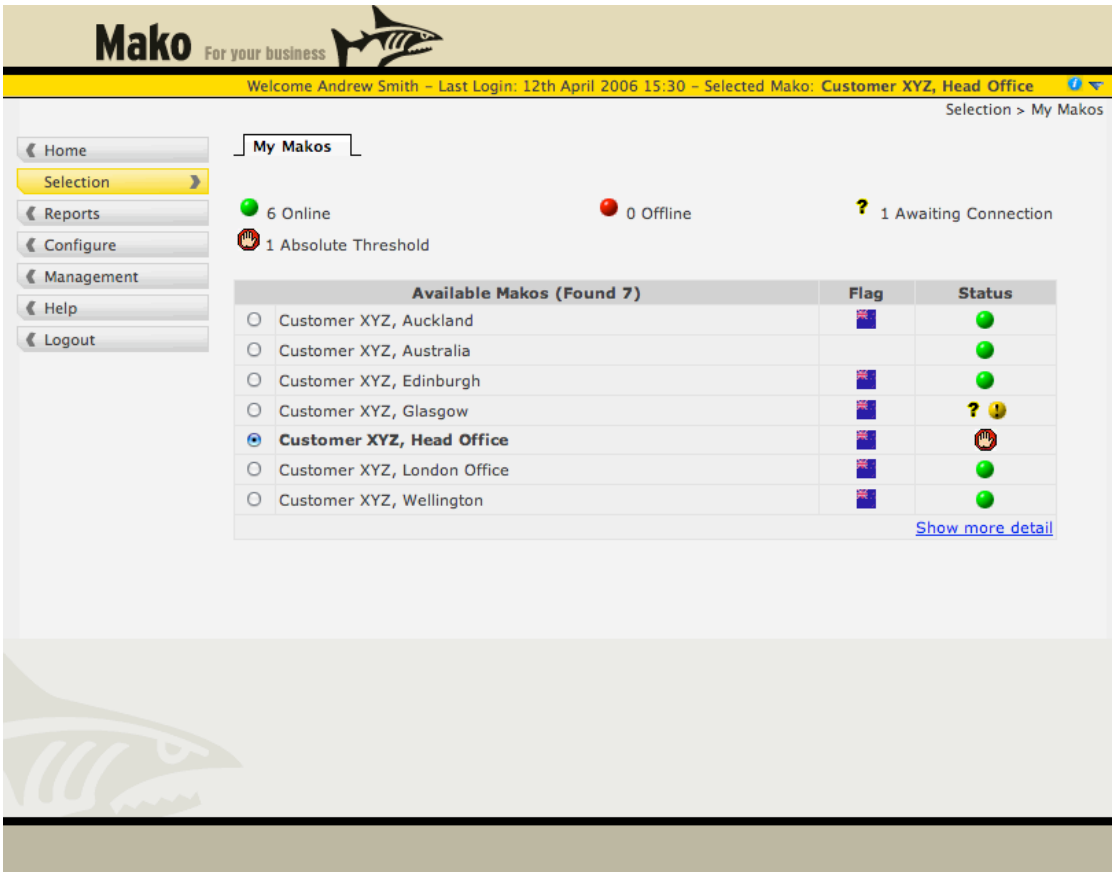
Selection screen

This screen shows the Mako units you are registered as using, and allows you to select sub-menus for Reports, Configuration and Help as described below depending upon the agreement between you and your IT professional. You can also see what country the Makos are located in and their Online/Offline/Awaiting Connection status. If any of your Makos have reached their Absolute Traffic Threshold, this will be shown as in the example depicted above for the Head Office Mako.

First, select which of your devices you wish to work with. Click on the radio button next to the device you wish to choose in the central box. Depending on your browser you may get an immediate response and the screen will refresh, or you may need to click on OK.

Once you have selected a Mako appliance you will see two new menus appear on the left side of the page: Reports and Configure. From these menus you can — obtain Reports, review or update the Mako appliance Configuration or add services.

Mako Appliance Selected
The chosen Mako appliance is now shown in the session status line, near the top right of the screen.

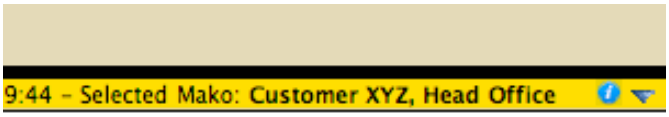


Selected Mako

Select your desired operation: Reporting, Configuration or Help by clicking on the required menu from the list on the left hand side.

The different operations are described on the following pages.

Quick Information Snapshot
There is an information "I" symbol near the top right of the page which gives you a snapshot of information about your selected Mako.



Information & Quick Selection buttons

Selection Shortcut
Next to the Information symbol is an upside down triangle. Clicking on this gives you a list of your recently selected Makos. This comes in handy when you are in other areas of the site and want to select another Mako or if you have a large number of Makos to manage.

Reports: Usage

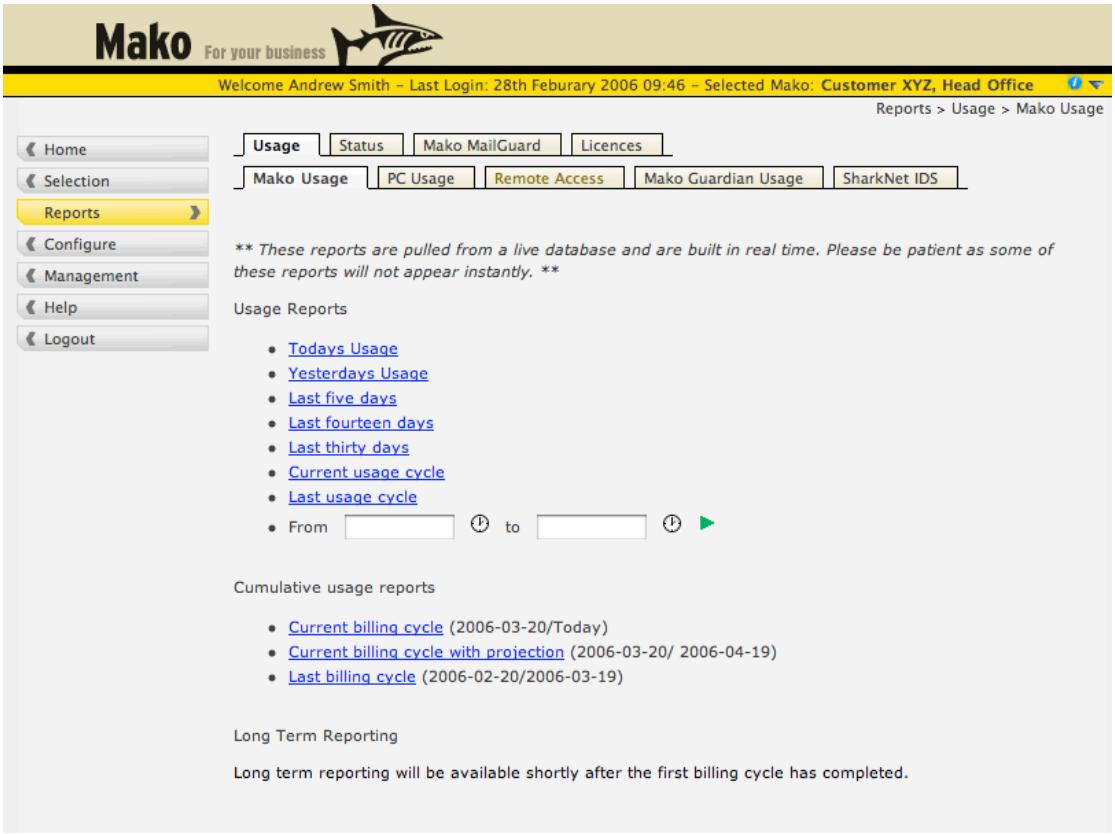
The Reports section provides a comprehensive array of options for displaying analysis of the traffic that has flowed through the Mako device.

Reports let you review traffic usage:

- As snapshots or cumulative use over different time spans, taken for your network as a whole;
- Similar reports, this time for traffic related to a particular PC in your office, to which you can assign a name;
- Detailed PC reports, which review a PC's traffic in relation to the type of traffic (protocol) and the remote site (destination) of the communications.

You are also able to check on the status of your Mako appliance.

Mako Usage
This section allows you to obtain a selection of reports from the chosen device. The options available are shown in the example screen below.



Reports, Mako Usage

Examples of typical reports are shown on the following pages

Considerations
Mako Usage refers to the total traffic which has passed through the Mako device. These reports therefore give you the sum total of your networks Internet usage, broken down into the listed time periods. You can drill down by day hour or PC by clicking on the appropriate parts of the graphs.

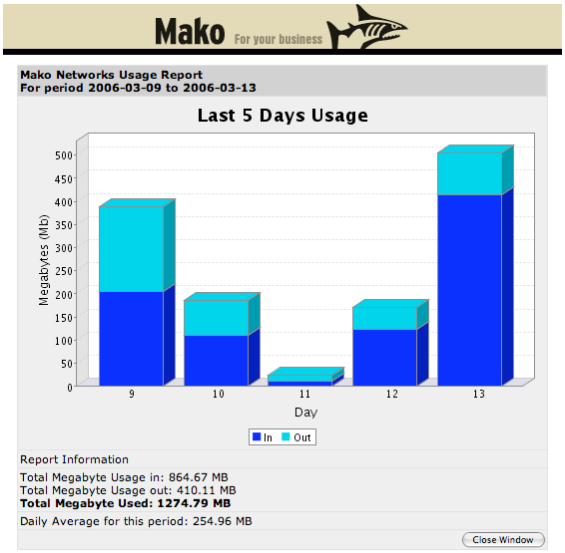
Usage cycle time periods commence at the Billing Cycle Start Date set in the Internet configuration section.

Usage Reports are displayed as a column graph in a pop-up window. The columns show incoming and outgoing traffic for each day in the selected time period.

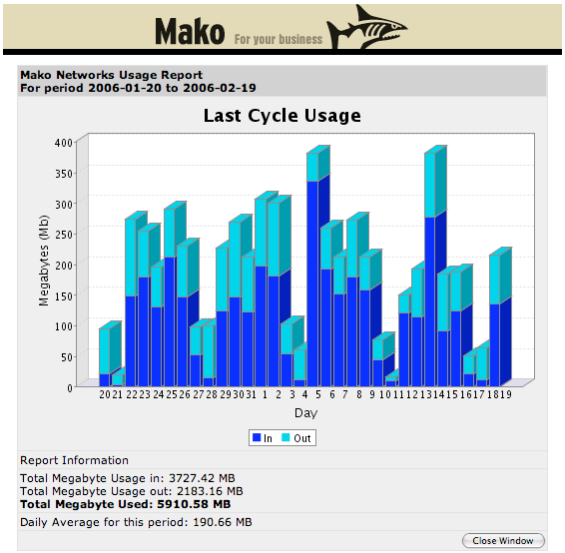
Cumulative usage reports are displayed as a line graph in a pop-up window. A line shows the sum of the accumulated incoming and outgoing traffic over the selected cycle.

In regions where traffic is billed on a usage/plan basis there are options available to set various thresholds. In the event that these are set up, up to three horizontal threshold limit lines can be displayed. The first shows the Traffic Warning Threshold value where you and your reseller will be emailed on the limit being reached. A second line shows the total amount of free traffic your ISP Connection Plan provides. The third shows the optional absolute threshold value where your firewall will disallow all incoming and outgoing traffic other than access to the Mako Networks Web Site where it can be re-allocated.

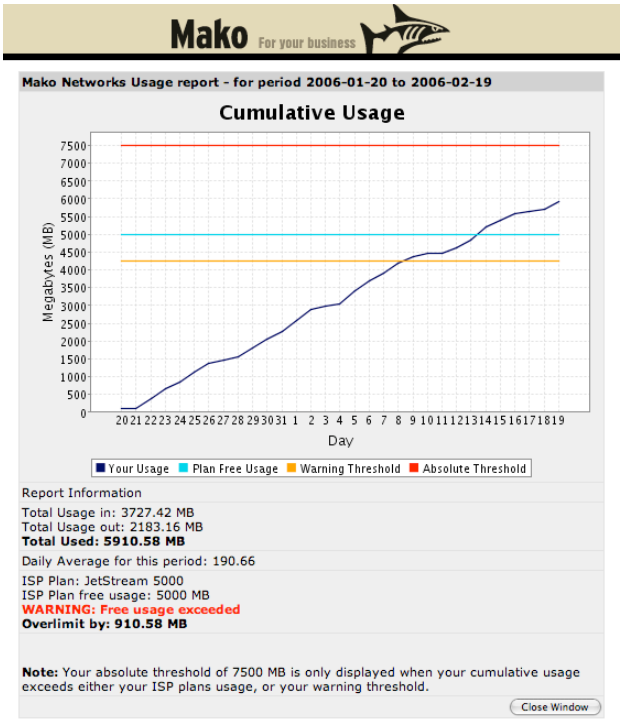
Please contact your reseller or ISP if you have any queries regarding your ISP charging structure.



Mako Report, Last Five Days



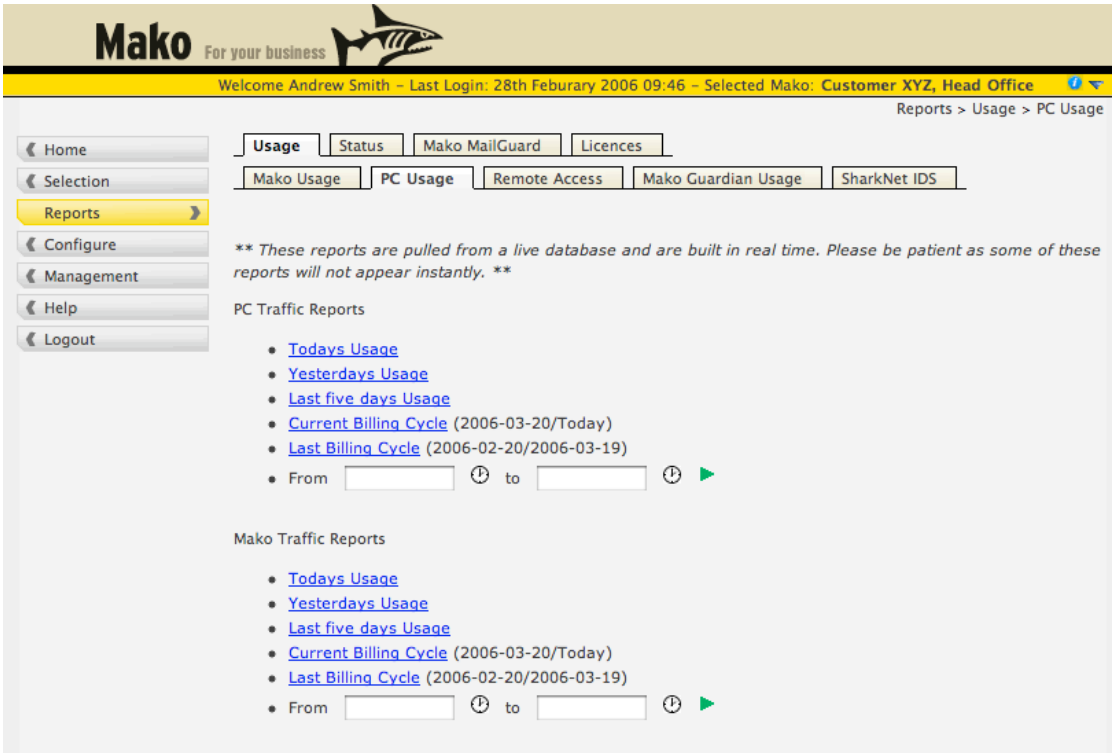
Mako Report, Last Cycle Usage



Mako Report, Last Billing Cycle

PC Usage
The PC Usage Reports focus on the composition of your traffic volume.

The entry screen to this section is shown below.



Reports, PC Usage

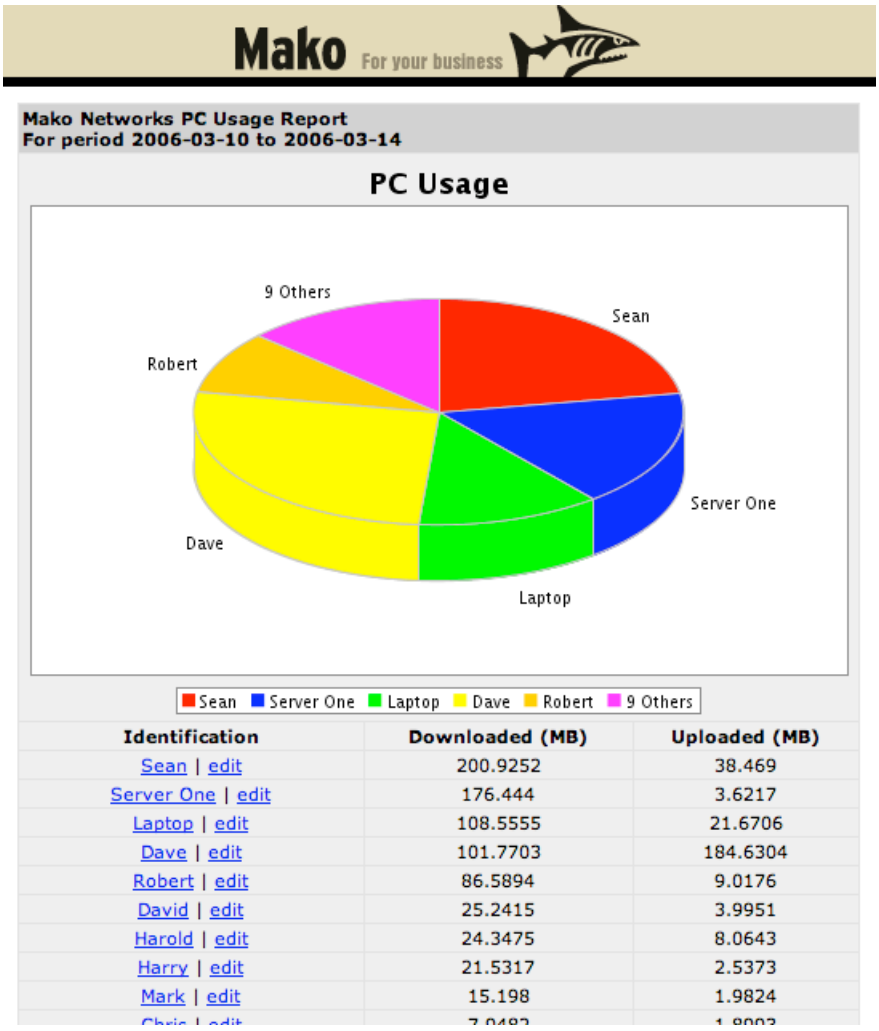
MAC Address & Naming PCs
Each PC on your network is assigned an IP Address to identify its communications. In many networks the network configuration allows the IP address to change from time to time. The IP address is thus not useful as a unique and unambiguous identifier over time for any particular PC.

Since reports show traffic over time, Mako uses the PC's MAC Address as a unique identifier. The MAC Address is rather cryptic, so to make reports more intelligible you can assign a name to each machine. This name will henceforth be displayed in your reports in place of the MAC Address.

If you click on 'edit' in a report a small pop-up window will be displayed. Enter the desired name in the box next to Machine Name and click on Update to save the name. Where PCs have been assigned static IP addresses via the Mako DHCP Server, a PC name can also be entered via the DHCP screen.

PC Traffic
PC Traffic reports let you analyse the network Internet activity to see the elements of traffic in relation to the individual PCs in the office. This is the place to look if you wish to see why a user has an exceptional load pattern for a given period.

Reports can be obtained for Today, Yesterday, the Last Five Days, the Current Billing Period, and the Last Billing Period. These reports are broadly similar, changing only by the amount of traffic that is analysed.



Identification	Downloaded (MB)	Uploaded (MB)
Sean | edit	200.9252	38.469
Server One | edit	176.444	3.6217
Laptop | edit	108.5555	21.6706
Dave | edit	101.7703	184.6304
Robert | edit	86.5894	9.0176
David | edit	25.2415	3.9951
Harold | edit	24.3475	8.0643
Harry | edit	21.5317	2.5373
Mark | edit	15.198	1.9824

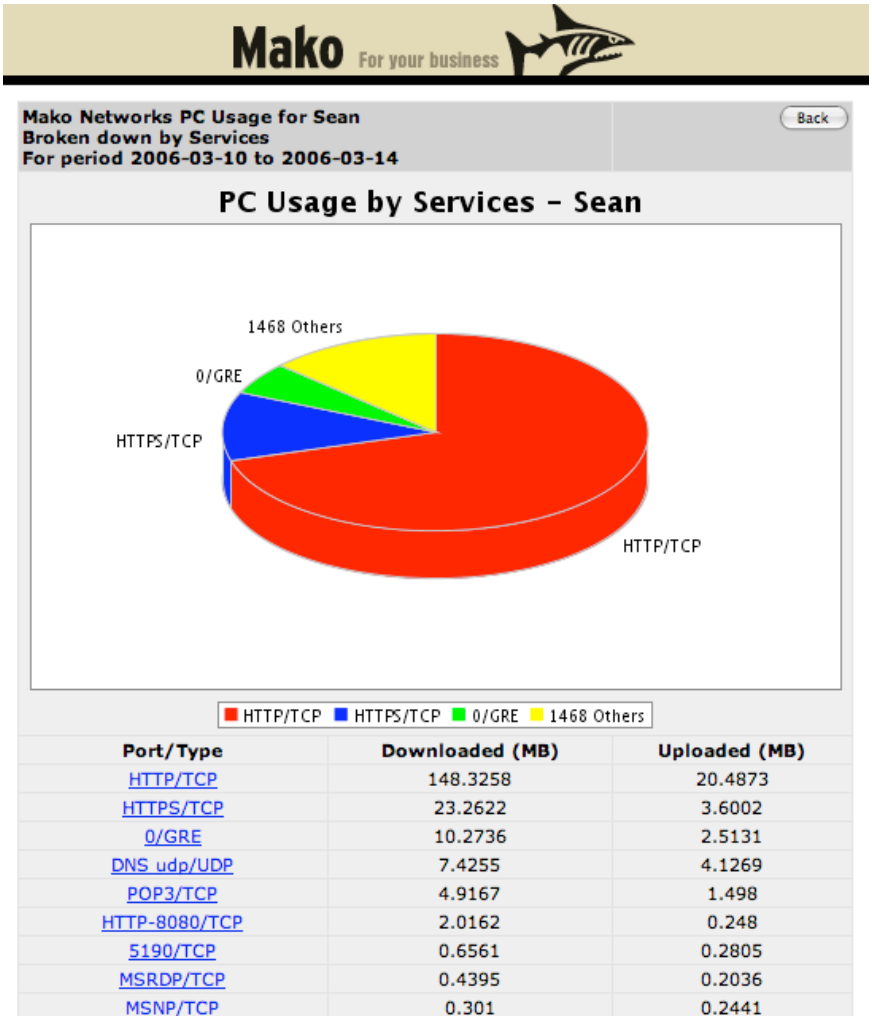
PC Usage, Last Five Days

The above screen shows an example PC Traffic report. Each device on the local network which has contributed to traffic flow in the selected period is listed under Identification. Alongside each entry is the volume of traffic Downloaded from (inbound) the Internet or Uploaded to (outbound) the Internet.

Note the 'edit' tab next to each name to permit the device to be given a more relevant name. Where a device has not been named the MAC Address will be shown. Clicking on 'edit' will pop-up the small window shown, which allows the name to be updated.

Clicking on the device name itself produces a new report, shown below. This report breaks down the total traffic for a device into the different services which contribute to the total. Each service is listed in the first column, headed Port/Type. Services are listed in descending order based on greatest volume first.

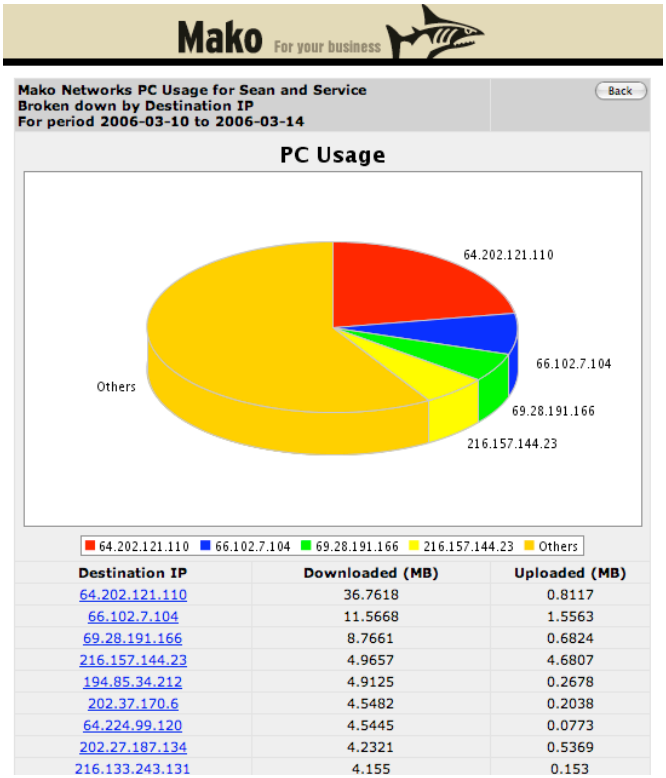
Services



Port/Type	Downloaded (MB)	Uploaded (MB)
HTTP/TCP	148.3258	20.4873
HTTPS/TCP	23.2622	3.6002
0/GRE	10.2736	2.5131
DNS udp/UDP	7.4255	4.1269
POP3/TCP	4.9167	1.498
HTTP-8080/TCP	2.0162	0.248
5190/TCP	0.6561	0.2805
MSRDP/TCP	0.4395	0.2036
MSNP/TCP	0.301	0.2441

PC Usage by Services

A further analysis can be performed by clicking on one of the service protocols listed. In this example we will analyse the HTTP traffic (web browsing).



PC Usage, Service, HTTP

This breaks down the service by Destination IP address, that is, the Internet location with which the particular traffic was exchanged.

In our example the web browser traffic has been listed under all the web sites which were contacted during the selected report period, and the amount of traffic associated with each.

Each IP address in the list can be clicked on to bring up a small pop-up window. This details everything that the Mako appliance knows about the Destination.

If you click on the IP address in this small window a new window will be opened to the actual web site concerned.

Using this functionality you can drill down into the reports to determine exactly which web site a PC user connected to, to generate an item of download traffic.

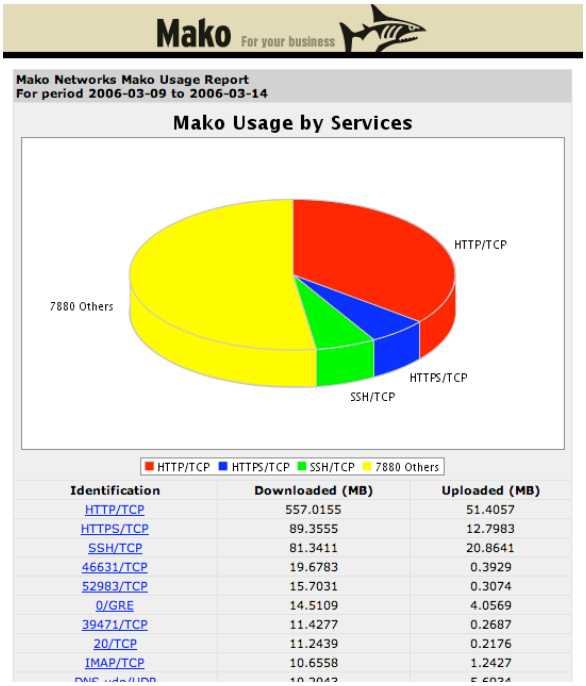
The reports incorporate hyperlinks to the Destination IP address, a convenient way to check on the type of downloaded information by simply opening a window at the web site. Detailed data on the amount and type of traffic relating to that web site is shown in the pop-up box.

- Click on the Destination IP address in the main report table to show the pop-up box.
- Click on either the IP Address or the Host Name in the pop-up box to open a window to the destination web site.

Mako Traffic

Mako Traffic reports let you see how a specific PC's Internet activity relates to other PCs on your network. This is the place to look to get a breakdown of the traffic by service (protocol, port) over a given period.

Reports can be obtained for Today, Yesterday, the Last Five Days, the Current Billing Period, and the Last Billing Period. These reports are broadly similar, changing only by the amount of traffic that is analysed.



PC Traffic, Mako Traffic

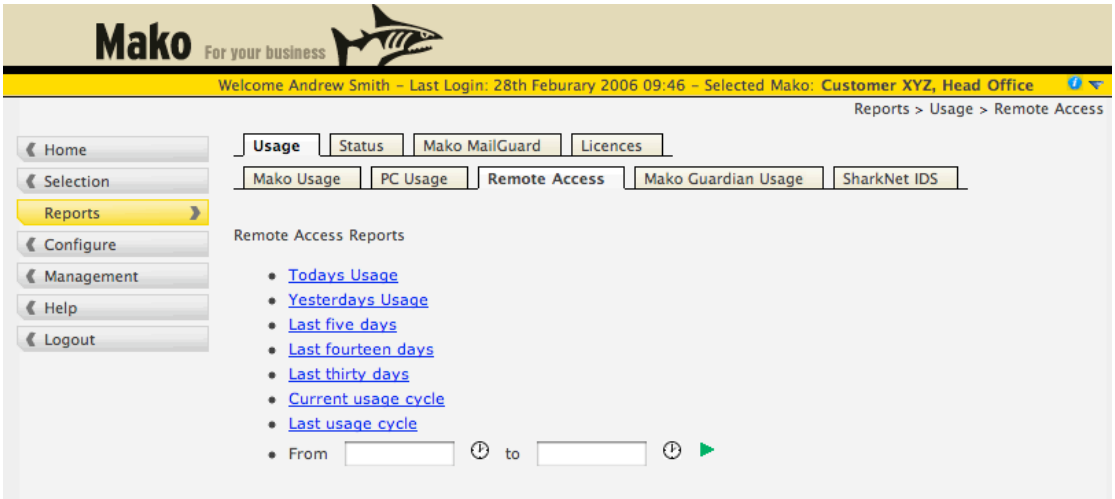
The screen above shows a comprehensive example of a Mako Traffic report, which is displayed in the pop-up window. A large number of services are permitted through this Mako device, each one of which is monitored.

Uploaded (outbound) and Downloaded (inbound) traffic volumes are shown by each of the services available, under Identification.

If you click on a service the pop-up window shows the PCs, which contributed to that service's traffic volume.

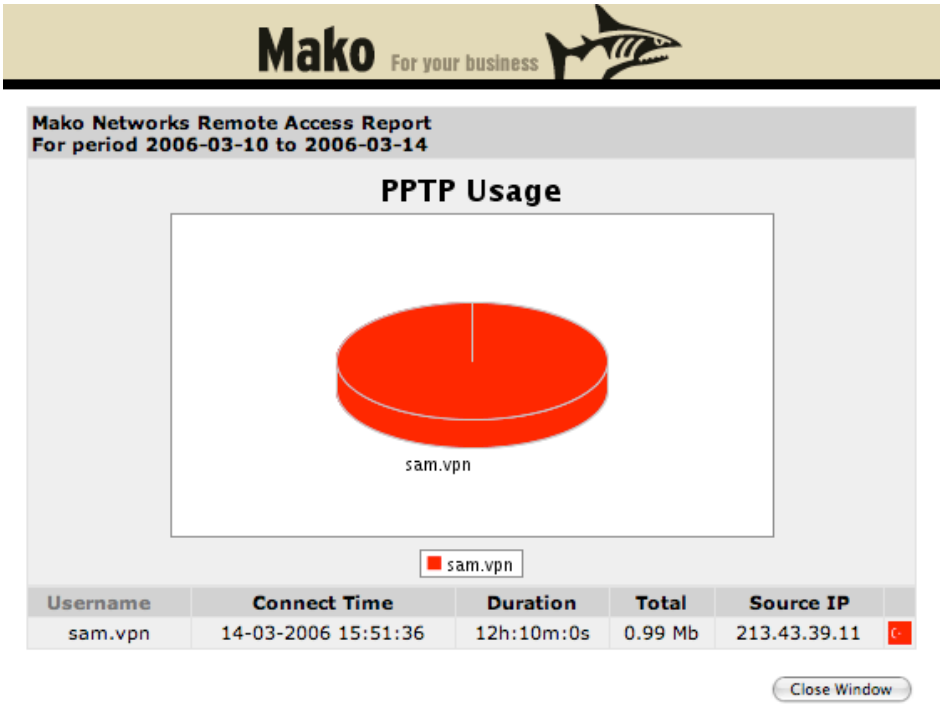
Remote Access

Remote access reporting gives you visibility over the PPTP Remote VPN users who connect to your Mako.



Remote Access Reports

Click on a period for which you would like to view details about PPTP connections. A popup window will display like the one below.



Remote Access Report

The Remote Access Report above shows which user(s) connected to your Mako protected network during the selected period. It also shows when they connected, for how long, how much data they transferred and where they came from.

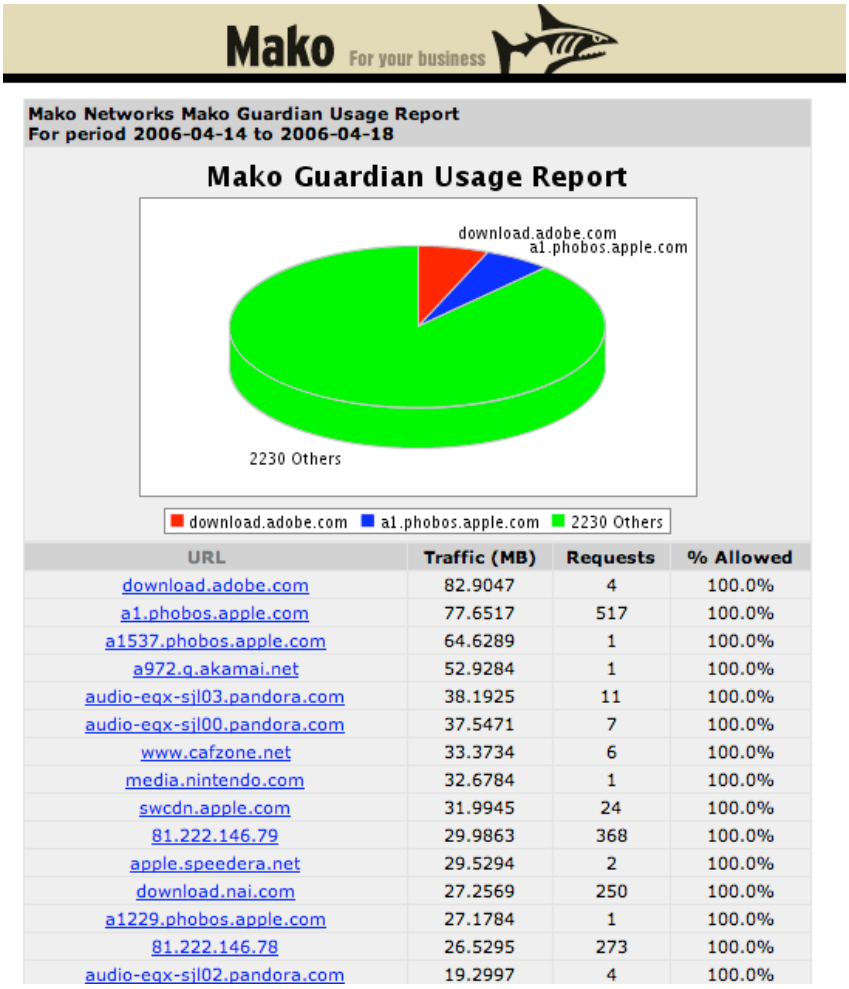
Mako Guardian Usage

Mako Guardian Usage is only visible if you subscribe to the Mako Guardian service. The Mako Guardian Usage reports display traffic volume by website visited.

Mako Guardian Usage Screen

By clicking on a period to view you will be shown the websites visited by computers on your network displayed by volume of traffic each site has contributed to your overall data throughput for the period.

Depicted in the example below are the websites visited by all the computers on a network over a five day period. The site download.adobe.com generated the most traffic and was visited four times. The % Allowed column shows if any aspects of the site were blocked for inappropriate content (in this example no blocks have been made on any of the visible sites).



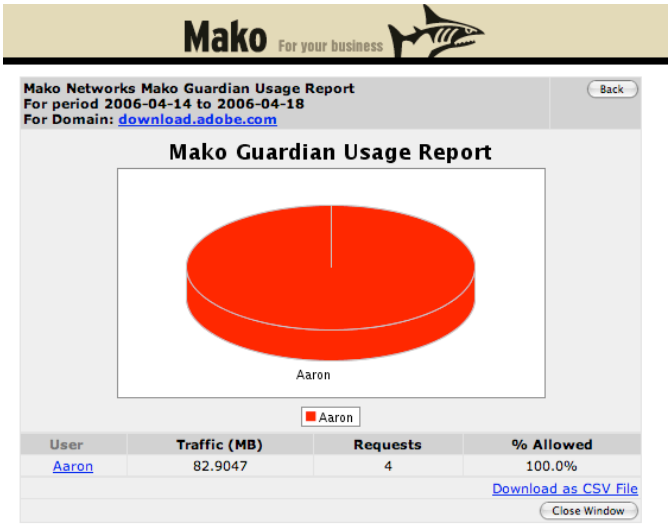
Mako Networks Mako Guardian Usage Report
For period 2006-04-14 to 2006-04-18

Mako Guardian Usage Report

URL	Traffic (MB)	Requests	% Allowed
download.adobe.com	82.9047	4	100.0%
a1.phobos.apple.com	77.6517	517	100.0%
a1537.phobos.apple.com	64.6289	1	100.0%
a972.g.akamai.net	52.9284	1	100.0%
audio-egx-sjl03.pandora.com	38.1925	11	100.0%
audio-egx-sjl00.pandora.com	37.5471	7	100.0%
www.cafzone.net	33.3734	6	100.0%
media.nintendo.com	32.6784	1	100.0%
swcdn.apple.com	31.9945	24	100.0%
81.222.146.79	29.9863	368	100.0%
apple.speedera.net	29.5294	2	100.0%
download.nai.com	27.2569	250	100.0%
a1229.phobos.apple.com	27.1784	1	100.0%
81.222.146.78	26.5295	273	100.0%
audio-egx-sjl02.pandora.com	19.2997	4	100.0%

Mako Guardian Usage Report

By clicking on one of the sites, another report will display who has accessed the site during the selected period.



Mako Networks Mako Guardian Usage Report
For period 2006-04-14 to 2006-04-18
For Domain: download.adobe.com

Back

Mako Guardian Usage Report

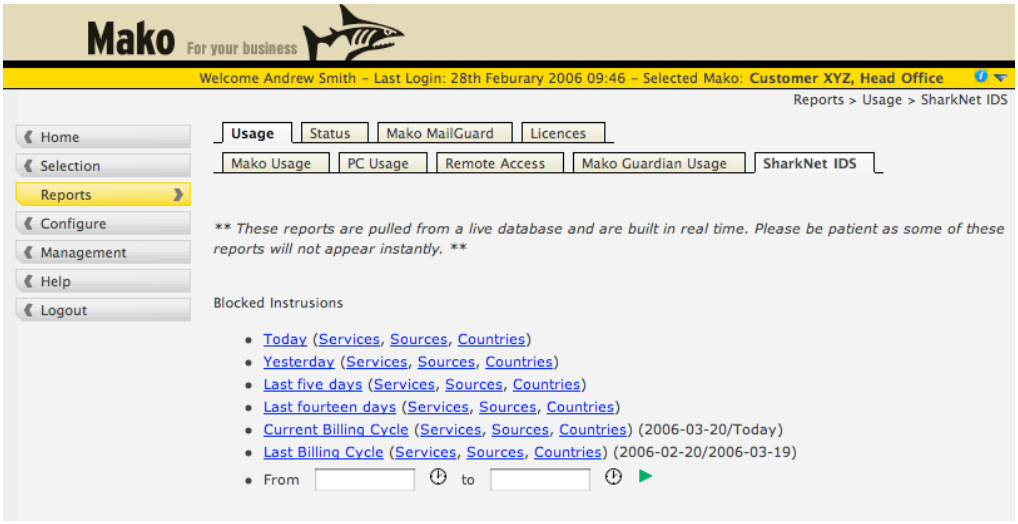
User	Traffic (MB)	Requests	% Allowed
Aaron	82.9047	4	100.0%

Download as CSV File

Close Window

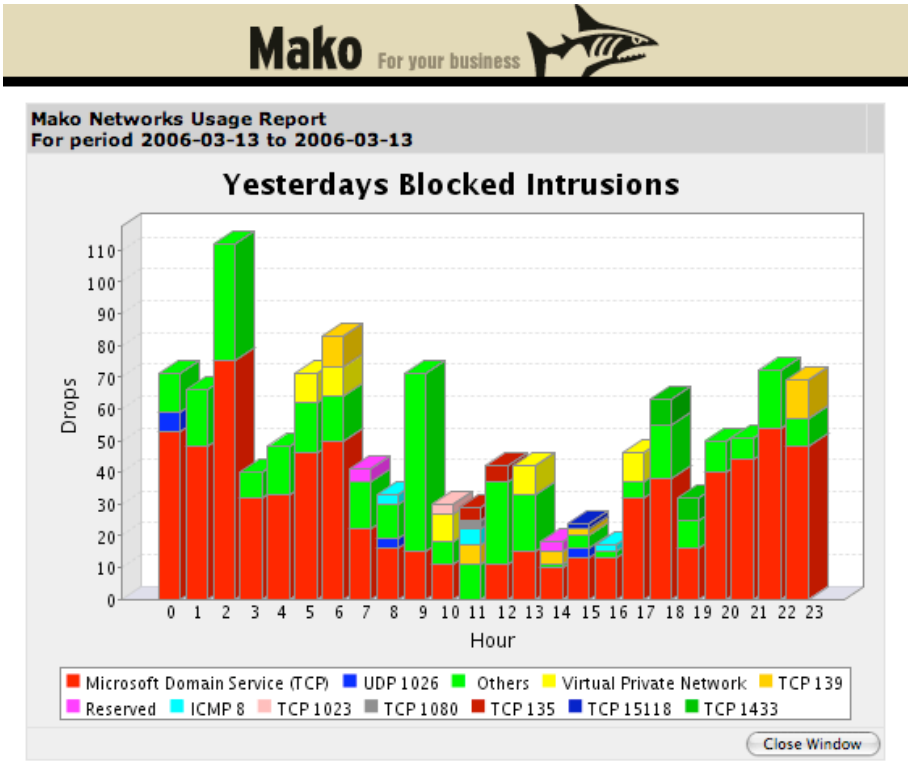
Mako Guardian Individual Site Usage Report

SharkNet IDS
IDS stands for Intrusion Detection Service. SharkNet IDS shows you what traffic has been blocked by the Firewall in your Mako device.



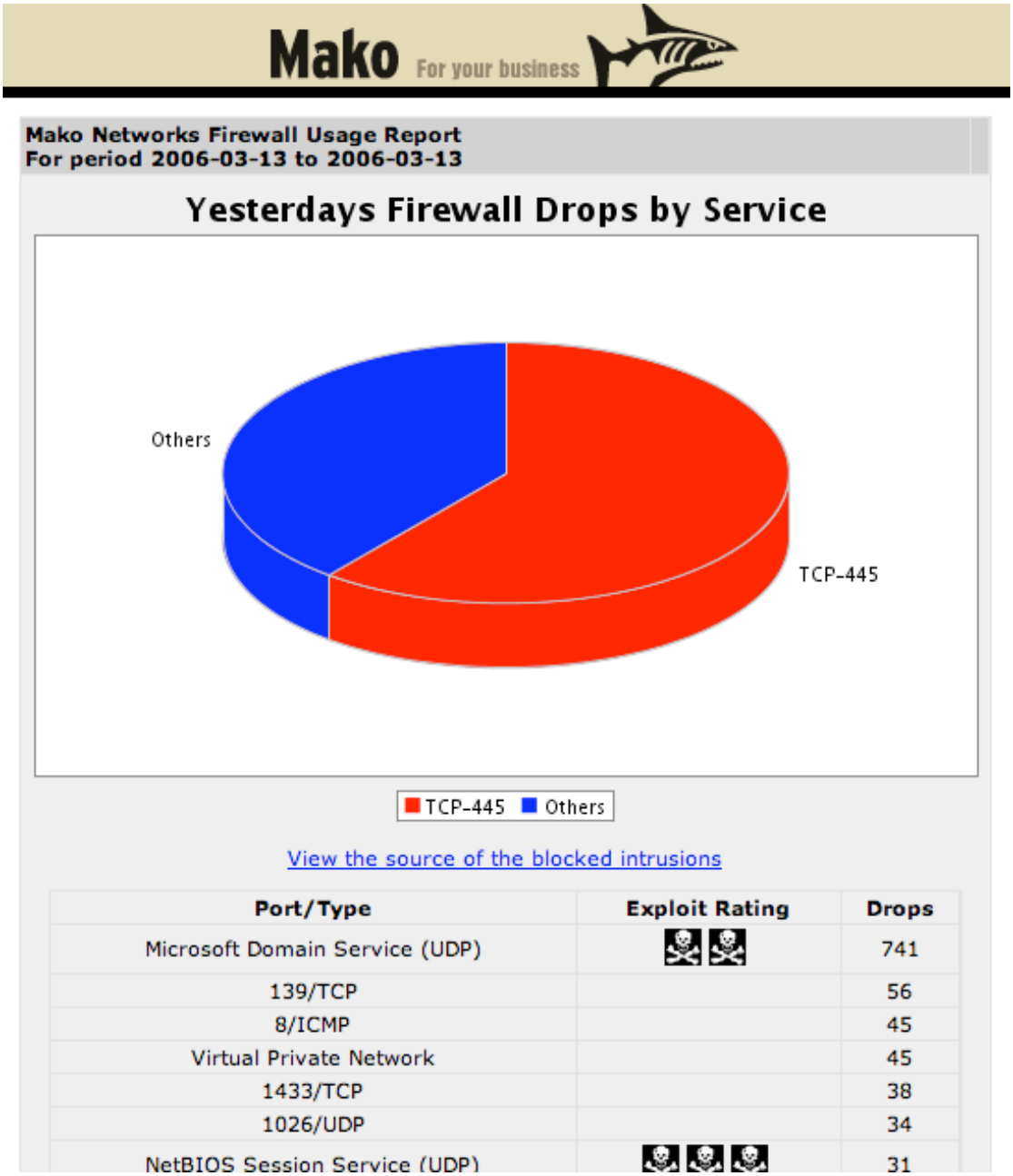
SharkNet IDS

SharkNet IDS lets you analyse what type of traffic is being blocked from entering your network, where is is coming from and how dangerous it is.



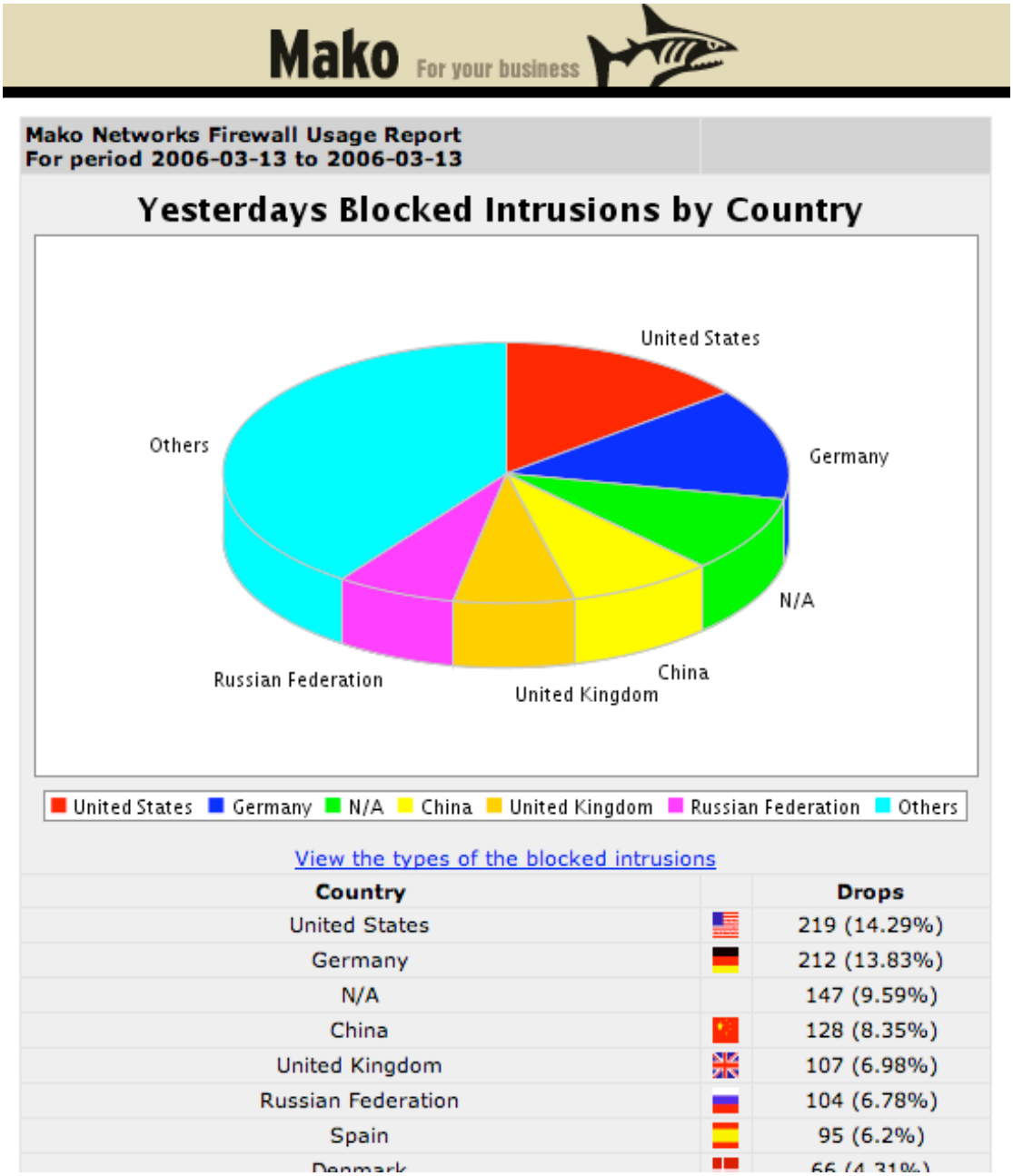
Blocked Intrusions for today

This report shows how many drops the Firewall made over the day so far broken down by hour. A key to the colours shows what type of traffic was dropped.



Firewall Drops by Service

This report show the same days IDS Report but this time by service. This depicts what type of traffic was dropped for the day so far. Below the pie chart the services are listed in order of most dropped to least. Some of the services have a number of skull and crossbones icons indicating the Exploit Rating of the service. The more skull and crossbones icons, the more “dangerous” the service that was dropped.



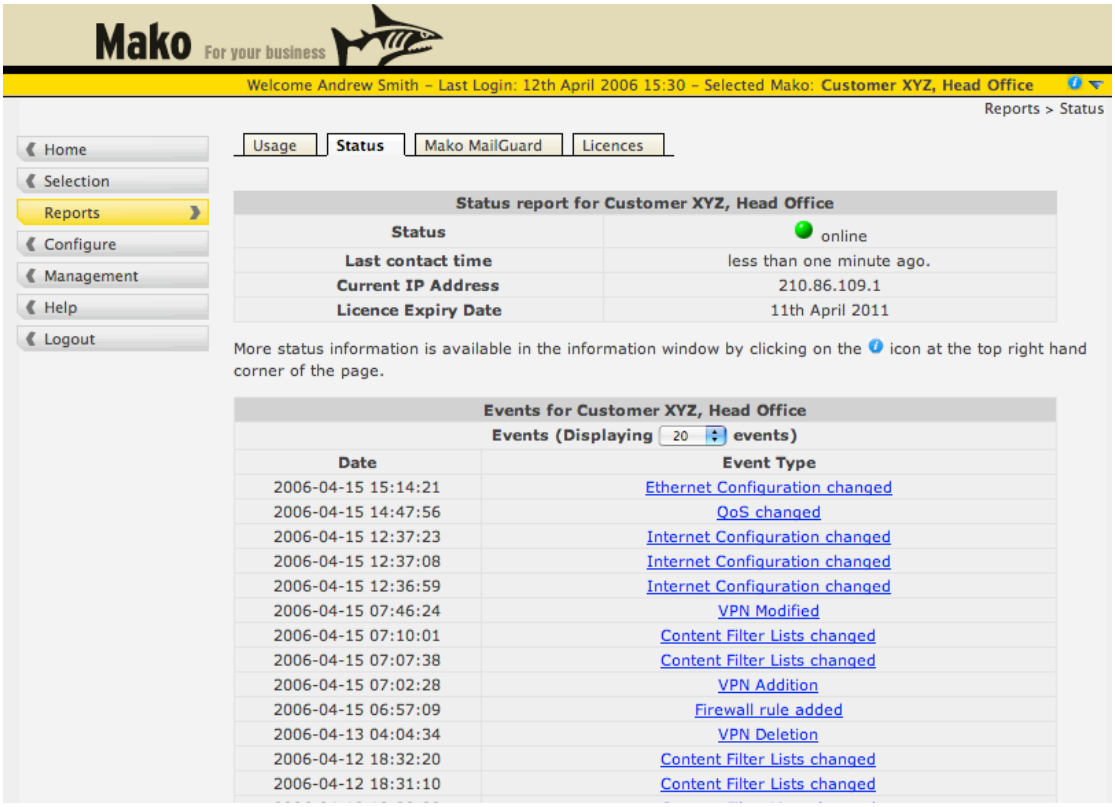
Blocked Intrusions by Country

This report shows where the intrusions that were blocked came from.

You can click on areas of most of the IDS report graphs and charts to drill down to find further information.

Reports: Status

This screen lets you check the status of the selected Mako device. It also shows the last user selectable number of events and the date of license expiry.



Reports, Status

Reports: Mako MailGuard

This tab is one way to access your Mako MailGuard console. If you do not subscribe to this service then this tab will not appear on your screen. Instructions on how to use the Mako MailGuard console appears in separate documentation.

Reports: Licence Information

The Licence Information screen allows you to keep track of your current Mako licences as well as add them when required.

Configure

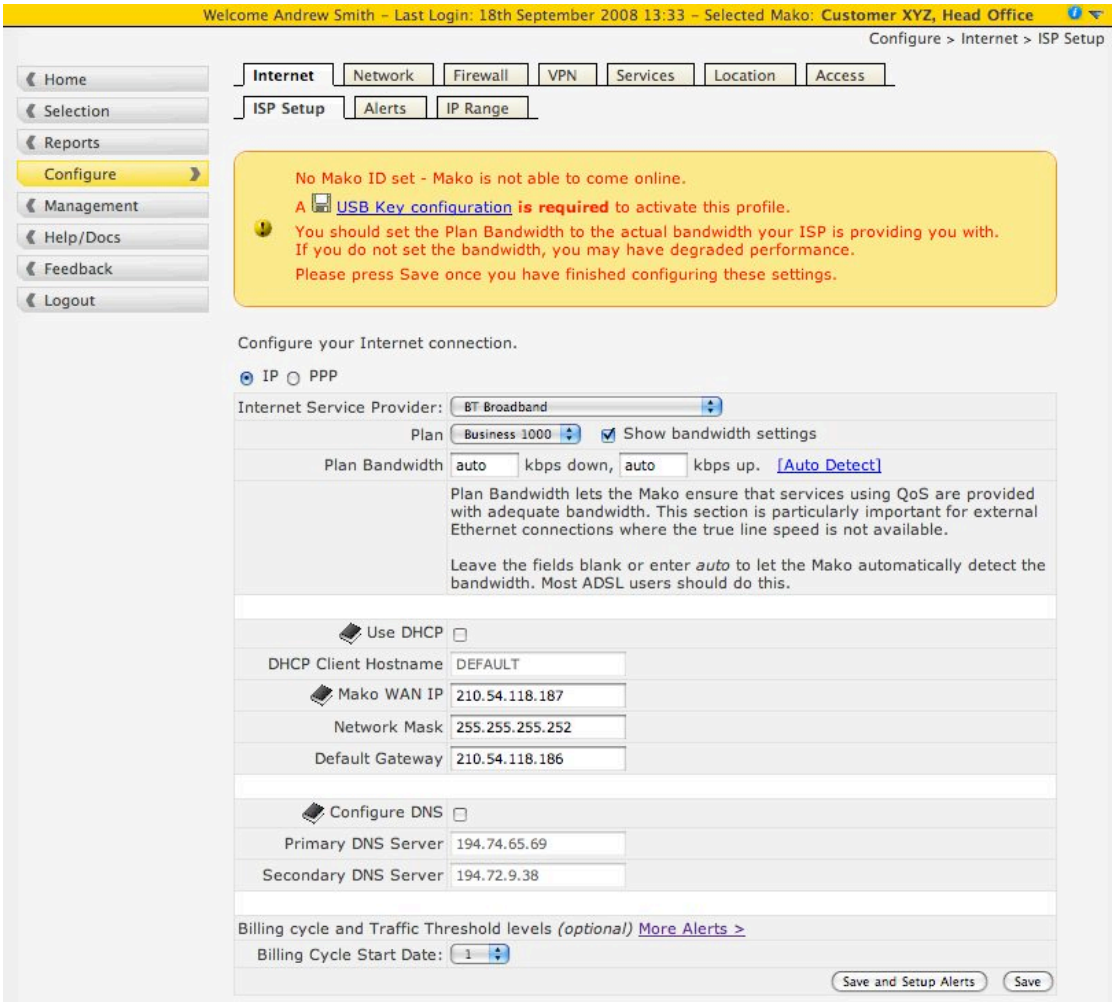
The configure section provides comprehensive options to update nearly every aspect of the Mako device. The default settings as shipped should be correct for your network. However over time new capabilities are often required. Your reseller can advise on the changes that are appropriate as your requirements change.

Please be aware that some of these functions can disable critical operations in your Mako device — care should be taken to ensure that configuration changes do not compromise your office network security or its access to the Internet.

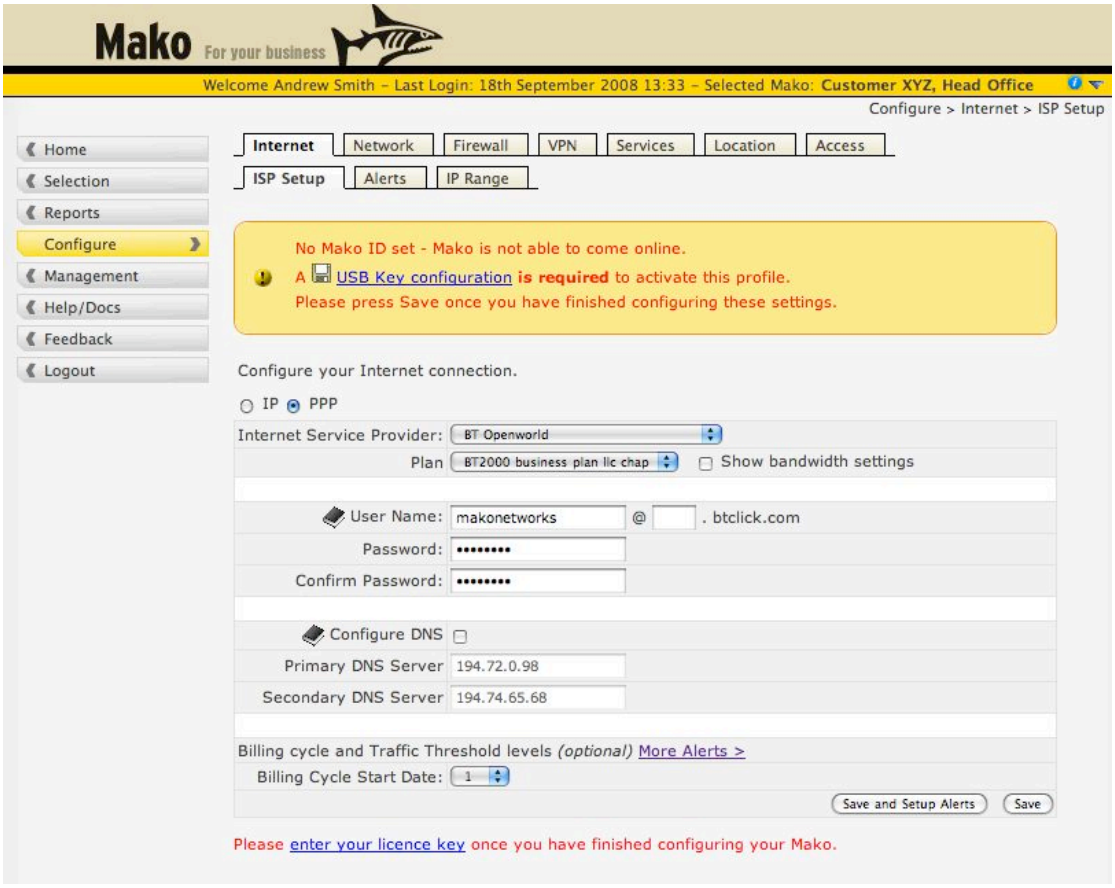
Configure: Internet

Internet
This screen allows you to review your Internet Service Provider access details and your traffic plan if you have one. The information on this screen will be set by your reseller and in most cases will never need to be changed. This screen could differ depending upon your ISP.

With a Mako 7550-E you can configure it using IP, DHCP or PPP (bridged Ethernet).



Internet Configuration - IP



Internet Configuration - PPP

If your ISP charges for traffic over and above a predetermined “plan”, you can set the Traffic Warning Threshold to a value of your choice, using the drop-down menu. You will be alerted when this percentage of your freely available traffic, according to your Connection Plan, has been reached. Set the Billing Cycle Start Date to that of your ISP agreement.

This facility is not available where your ISP Connection Plan does not impose a traffic charging threshold.

Your Mako appliance automatically detects computers on your network that are infected with worms and stops them from accessing the Internet. You can set how aggressive this detection is from this page.

Considerations
If you wish to change your ISP Password you must be sure to make the change at the same time with your ISP – preferably on their web site. Please be careful to type the password exactly the same at both places (Mako Networks and your ISP).

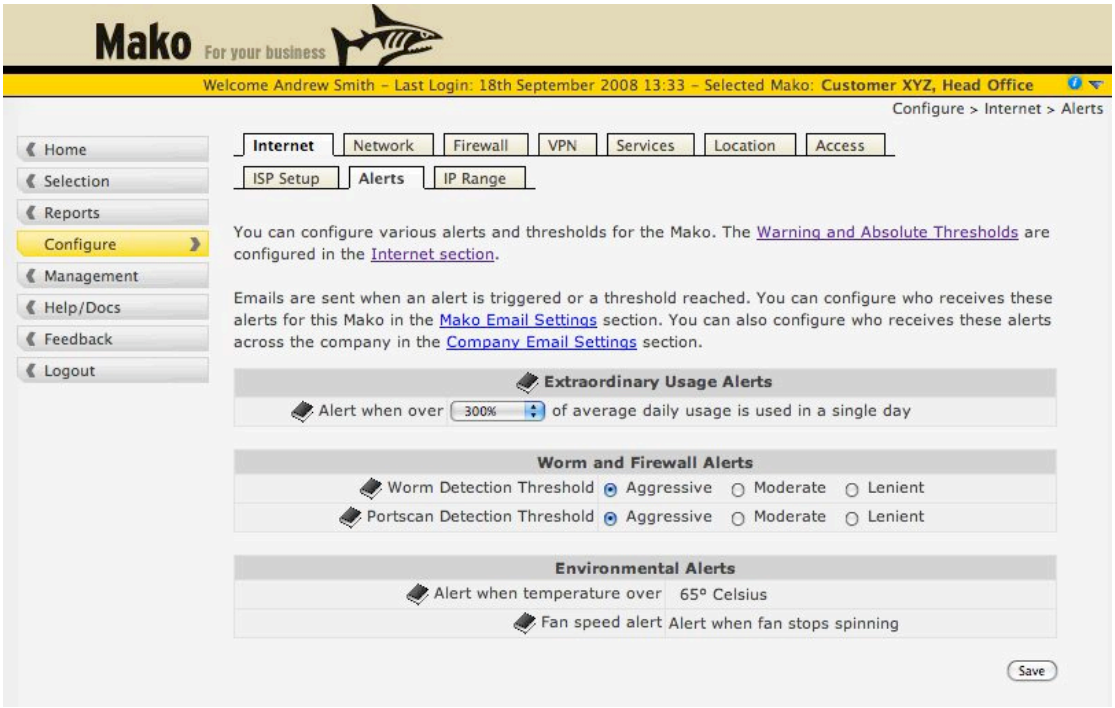
Click on OK to save your changes.

Alerts
The Alerts page allows you to set thresholds for alerting for extraordinary usage, worm and portscan intrusions and environmental conditions.

Extraordinary Usage alerts will trigger when traffic volumes reach the level you set. These alerts can be very useful in detecting abnormal usage quickly before it impacts your network or users.

Your Mako appliance automatically detects computers on your network that are infected with worms and stops them from accessing the Internet. You can set how aggressive this detection is from this page. Similarly, your Mako will detect unwanted portscan attempts and block the source IP Address for a ten minute period. You can set how aggressive this detection is from this page.

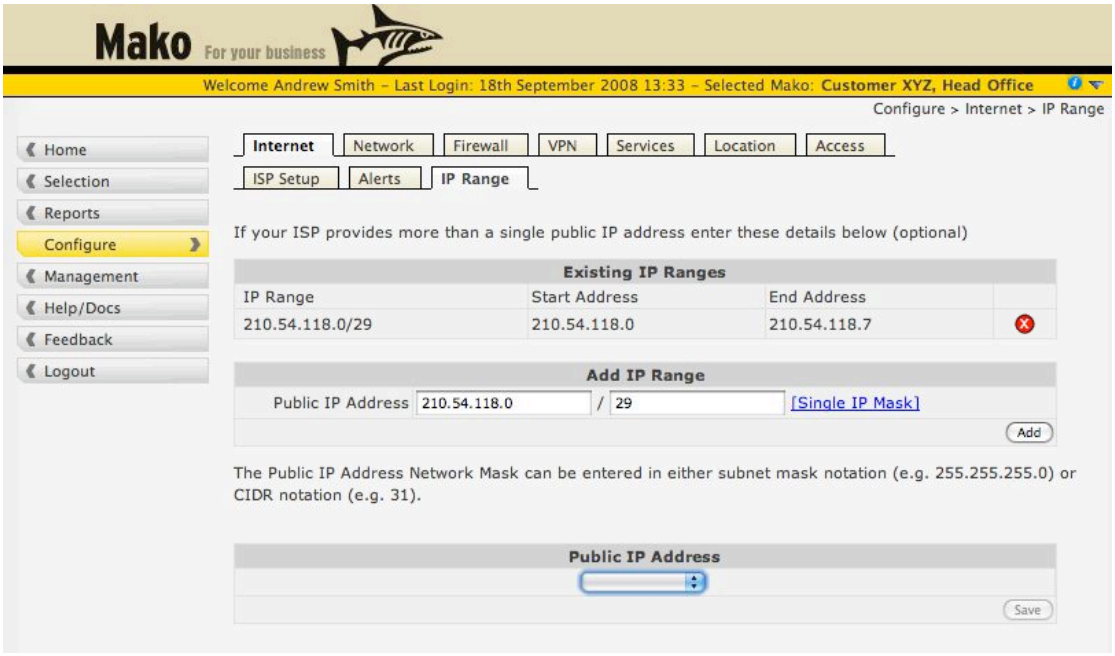
You can also choose at what CPU temperature you should be alerted at and whether you want to be notified if the fan stops spinning. The default settings for environmental alerts should only be changed in exceptional circumstances. Please consult your Reseller before making any changes to the Environmental Alerts.



Alerts screen

IP Range

This screen allows you to review your Public IP Address Settings if your ISP provides you with more than one. The information on this screen will be set by your reseller and in most cases will never need to be changed. If your ISP does not provide you with multiple IP Addresses, this screen will not be available.

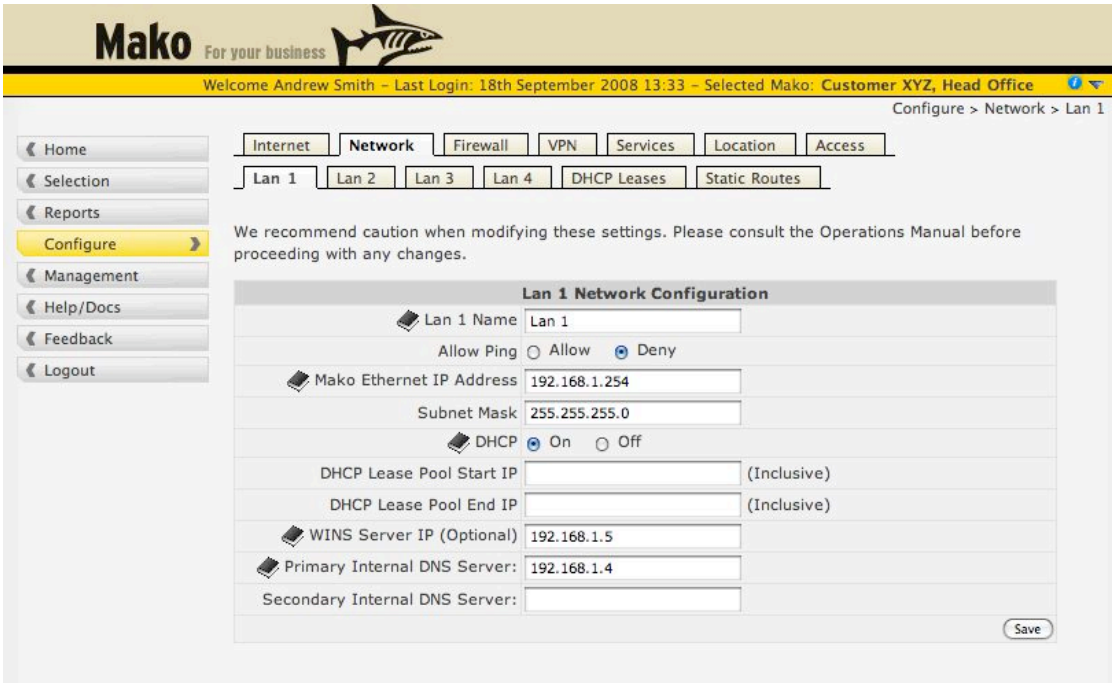


ISP Assigned Public IP Range

Configure: Network

Normally, this section will be configured by your reseller and no changes will be necessary. It is important that any alteration of the information recorded on this screen is done with care, as your communications with the Internet may be disabled if an error is made.

Lan 1



Network, Lan 1 Configuration

You may rename your network from Lan 1 to a more meaningful name (such as Office Network) if desired.

You can choose to allow the Mako to respond to ICMP (ping) traffic on its LAN 1 interface by selecting the Allow radio button.

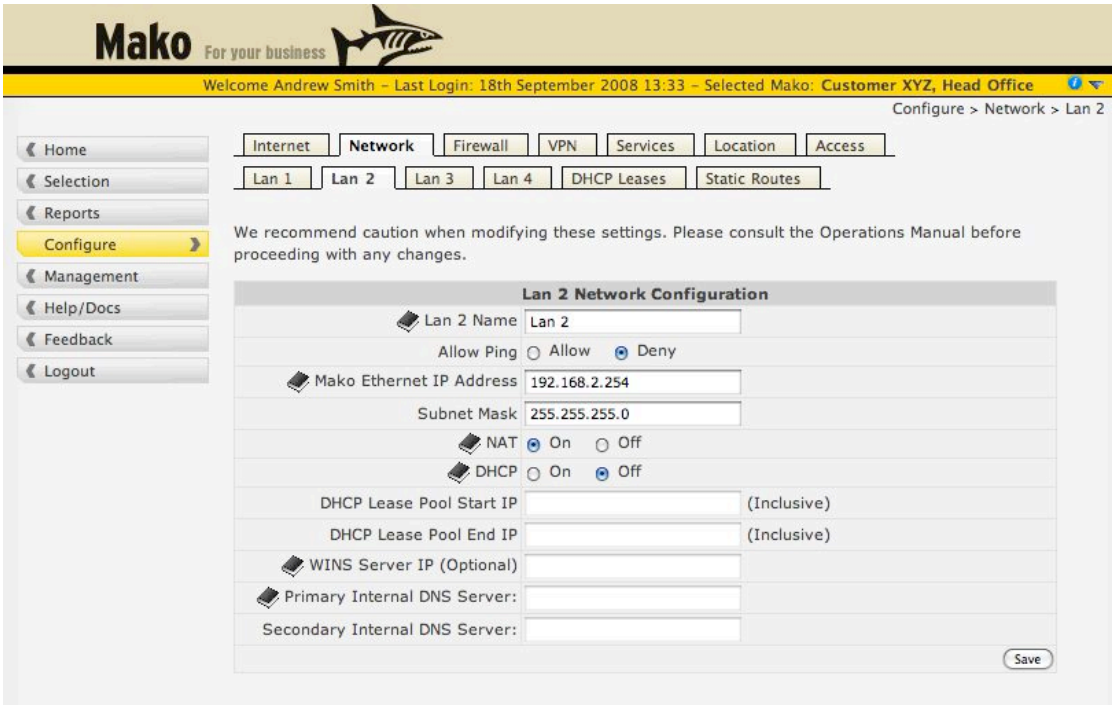
If your office network requires the Mako to provide DHCP functionality, the corresponding button should be clicked. You can specify a pool of IP Addresses that will be issued by the Makos DHCP Server.

You have the option of specifying a WINS server if this is required. You may also specify any internal DNS Servers. These are different from the public DNS Server addresses specified in the Internet configuration section.

The Mako device must be given a fixed IP address on your network. This is set to a default value (of 192.168.1.254 for your first network, 192.168.2.254 for your second, etc). It can be changed to suit the private address architecture used on your networks. It must not be set to a public IP address. You may also change the Subnet Mask address.

Please note that each network should be given a unique address schema if VPN communications are to be configured.

Lan 2, 3 and 4



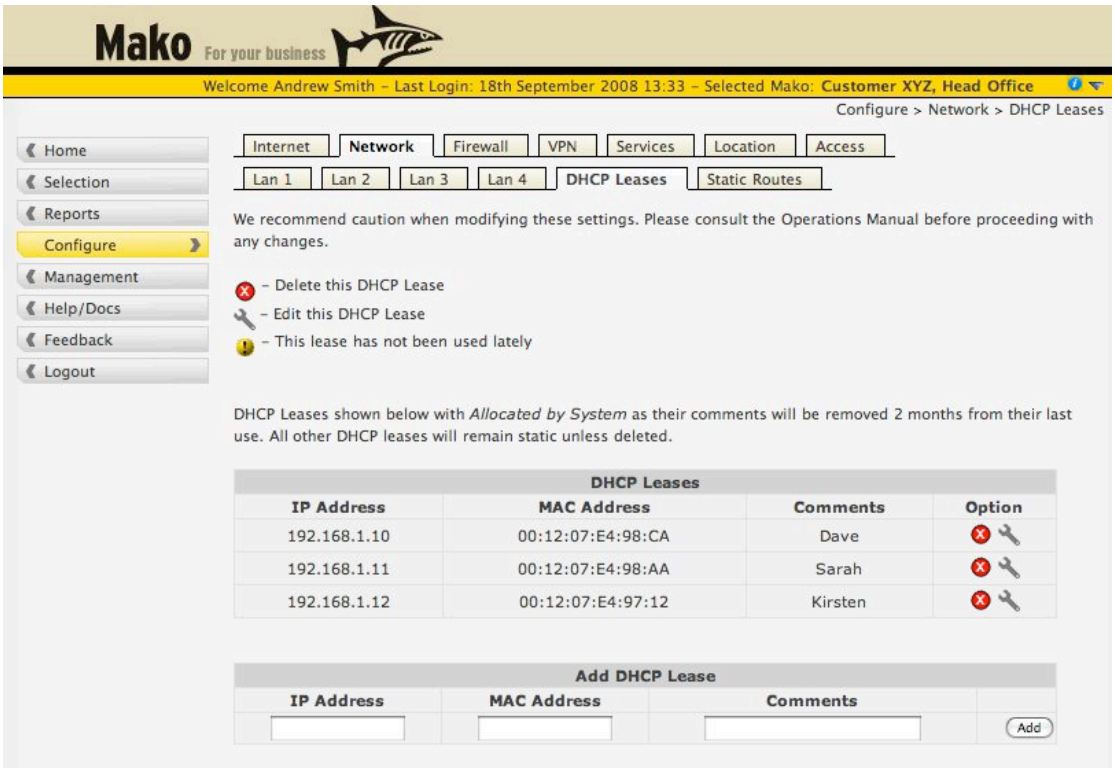
Network, Lan 2 Configuration

You may rename your network from Lan 2 (or 3 or 4) to a more meaningful name (such as DMZ) if desired.

The Mako device must be given a fixed IP address on your network. You may also change the Subnet Mask address.

The configuration is the same as for LAN 1 with the exception of being able to turn off Network Address Translation (NAT) if you have been issued with a public IP network by your ISP and you wish to use this public network on your LAN 2, 3 or 4 networks.

DHCP Leases
Normally this section will be configured by your reseller and no changes will be necessary. It is important that any alteration of the information recorded on this screen is done with care, as your communications with the Internet may be disabled if an error is made.



DHCP Leases

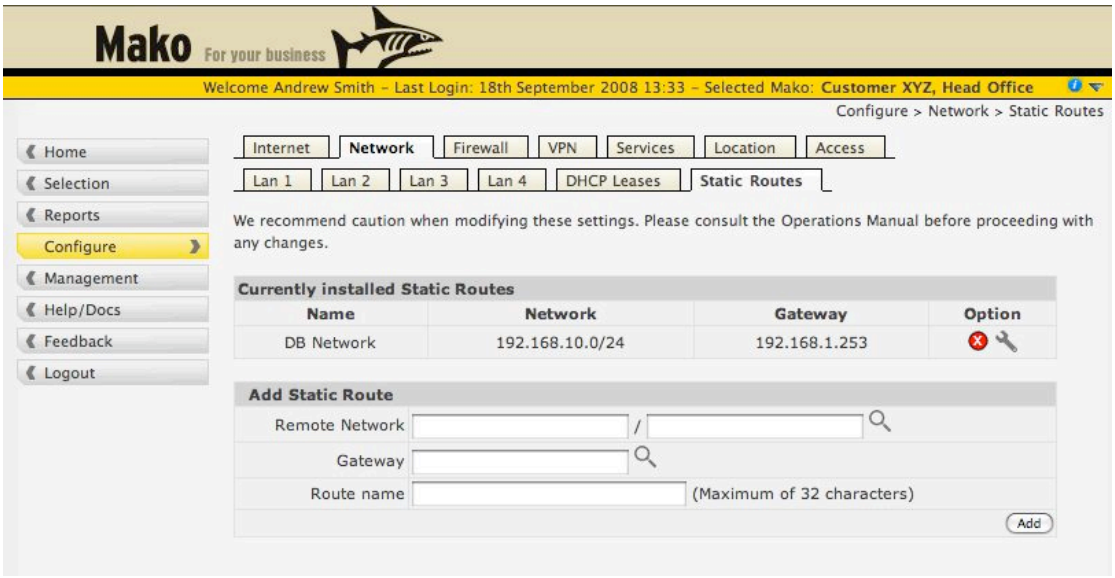
When the Mako's DHCP Server is enabled it will issue IP information to all PCs on the network.

Each PC computer has an Ethernet card for connection to the network. These cards are known as NICs. Each NIC has a unique, permanent MAC address. By associating the IP address with the MAC address we ensure that DHCP Leases for these machines are pre-defined. The Mako will always issue the same IP Address to a known MAC address.

To add a static IP address, enter details in the lower table and click on Add. The entry will appear in the table above as a static IP address. To remove an existing entry, click on the corresponding Delete button. The comments field allows you to enter an easily identifiable name for the PC. This will be carried over into the reports to simplify tracking usage.

Static Routes
Normally this section will be configured by your reseller and no changes will be necessary. It is important that any alteration of the information recorded on this screen is done with care, as your communications with the Internet may be disabled if an error is made.

You may enter routes to other networks that have routers on one of your LANs.



Static Routes

Configure: Firewall

The default security configuration for a Mako is to permit no communications initiated from the Internet to penetrate your networks. At the same time all communications initiated from the office network can access the Internet. In telephone terms, you can call out, but they can't call in.

This means that users on your Mako-protected networks can send and receive their email, browse the World Wide Web, and access all other Internet based services, while the firewall ensures that none of their PCs are visible to the Internet.

This is a very secure setting of your Mako device and should not be changed except in cases of specific need. Changes to permissions which Deny access tend to improve firewall security. Changes which Allow access tend to weaken firewall security. Changes to permissions should therefore specify the permitted access as narrowly as possible to minimise risk of unauthorised intrusion.

Inbound
This relates to the firewall rules which permit communications to be initiated from the Internet into your local networks by a remote host computer.

It is important to understand that Inbound access permissions place some responsibility for security of the local network onto the designated target local network PC or server. The firewall will pass through all communications matching the access permissions. If the local PC or server is not itself secure then other computers in the office network can be exposed to unauthorised access.

It is therefore sensible to exercise caution when enabling Inbound access. It is also necessary to ensure that target computers on the local network have all security related updates applied to their software.

Outbound
This relates to the firewall rules which permit communications to be initiated from computers in your office network to remote host systems on the Internet.

It is sensible to appreciate that, though the firewall will ensure that communications are only initiated by PCs on the local network, once established these communications are two-way. Internet based attackers have developed a wide variety of malicious software programs which can be downloaded onto a PC without the PC user's knowledge. These programs are generically known as 'Viruses', though other terms such as Trojan and Worm are in use.

The actions of virus programs can be very dangerous to your office computer systems. Early examples tended to perform obvious destructive acts such as the deletion of crucial system files. More recently information has been extracted by the virus to damage reputations by sending malicious emails under the name of the PC owner. Other varieties of virus may instigate industrial espionage with confidential information, may use office PCs in an Internet borne attack on a third party, or may steal Internet access at the office's expense.

The firewall is not a substitute for effective virus protection, which should be installed on all computers with Outbound access to the Internet, and which must be kept up to date at no less than weekly intervals.

Intranet
Mako 7550s have quad LAN ports and the Intranet firewall controls enable you to restrict or allow access between the four networks. The default setting is to not allow any communication between the four networks.

VPN
In addition to having control over inbound and outbound traffic, your Mako enables you to have firewall control over your Mako to Mako VPNs. To find out more about Mako to Mako VPNs, please see the VPN section of this document.

Once your Mako to Mako VPN is in place, with Mako VPN Firewall controls you can control the flow of traffic from one securely connected remote network to another.

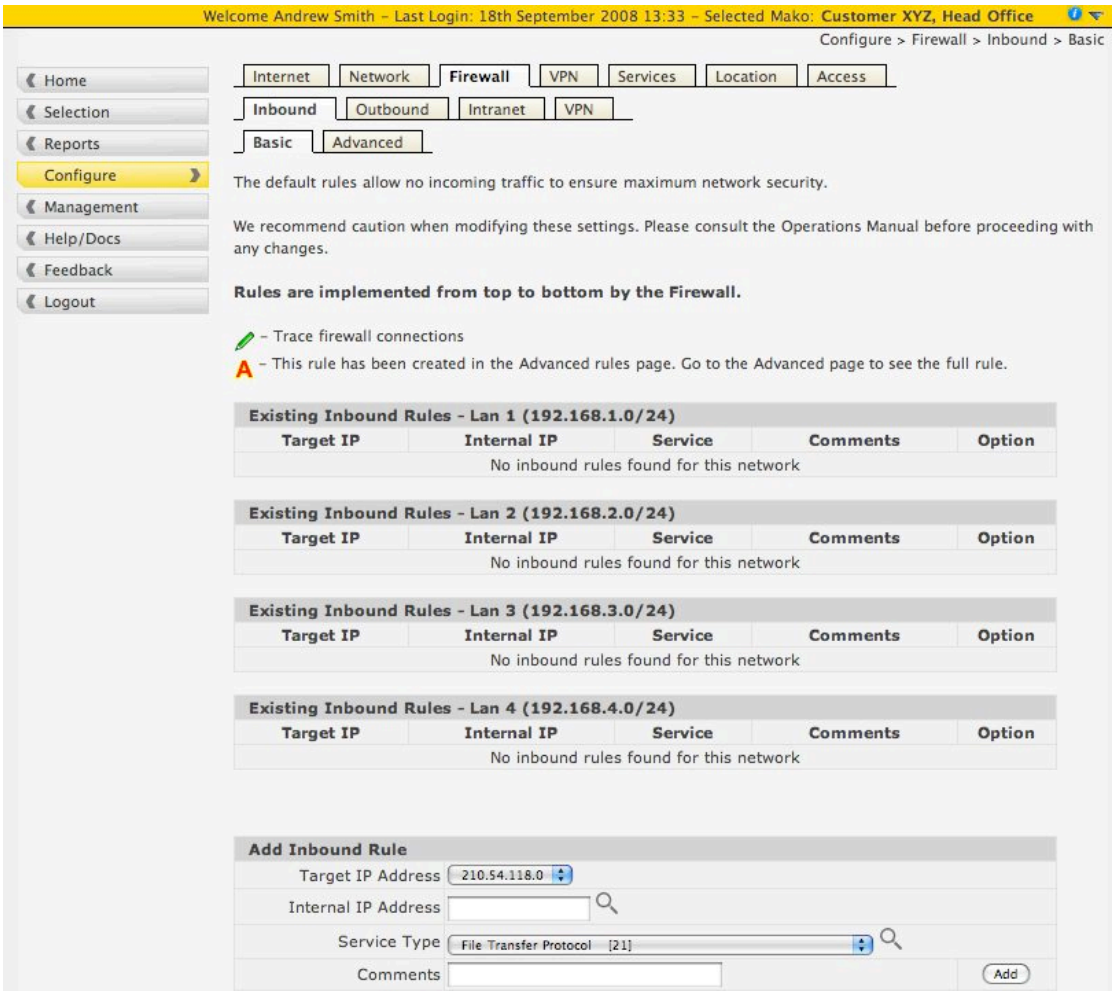
Considerations
If you plan to change the default security setting of your firewall there are some things it is useful to be clear about in preparation for the changes:

- Whether you are changing Inbound or Outbound firewall rules.
- Associated with this is whether you are Denying or Allowing access.
- The Service you wish to change access permissions for. A Service, such as email or web browsing, is defined as a specific Protocol, such as SMTP for email, or HTTP for unsecured web browsing. Each Protocol is uniquely distinguished on the Internet by assigning it a Port number. (e.g. SMTP is Port 25, HTTP is Port 80.) Port numbers in the range 0 to 1024 are assigned under international standard, while those above 1024 (up to 65,535) can be assigned by the Protocol publisher and are known as 'ephemeral' ports.
- The IP address(es) of the Internet hosts. In some cases you may wish to change access for all Internet based hosts rather than specifying individual hosts.
- The IP address(es) of the local PCs. Where particular local machines are to have their Internet access re-defined, it is necessary to ensure that each ones IP address is constant, or static. Please refer to the DHCP section for details of this procedure. This is not necessary when you are changing access for all PCs on your local network.

NB: Changes made can take up to two minutes to apply to your Mako. If you want a change to apply immediately, click on the Perform Refresh button at the bottom of the Firewall pages.

Inbound: Basic
Inbound Security is by default set to Deny all access initiated by hosts from the Internet. Please review the earlier discussion for background information on the issues involved.

There are a few occasions when an Internet based host needs to initiate communications with a PC on the office network. A common example is when a mail server is located in the office network, inside the firewall. It is frequently necessary for the mail server to receive incoming connections from mail hosts on the Internet, and this requires an access path through the firewall to be set up.



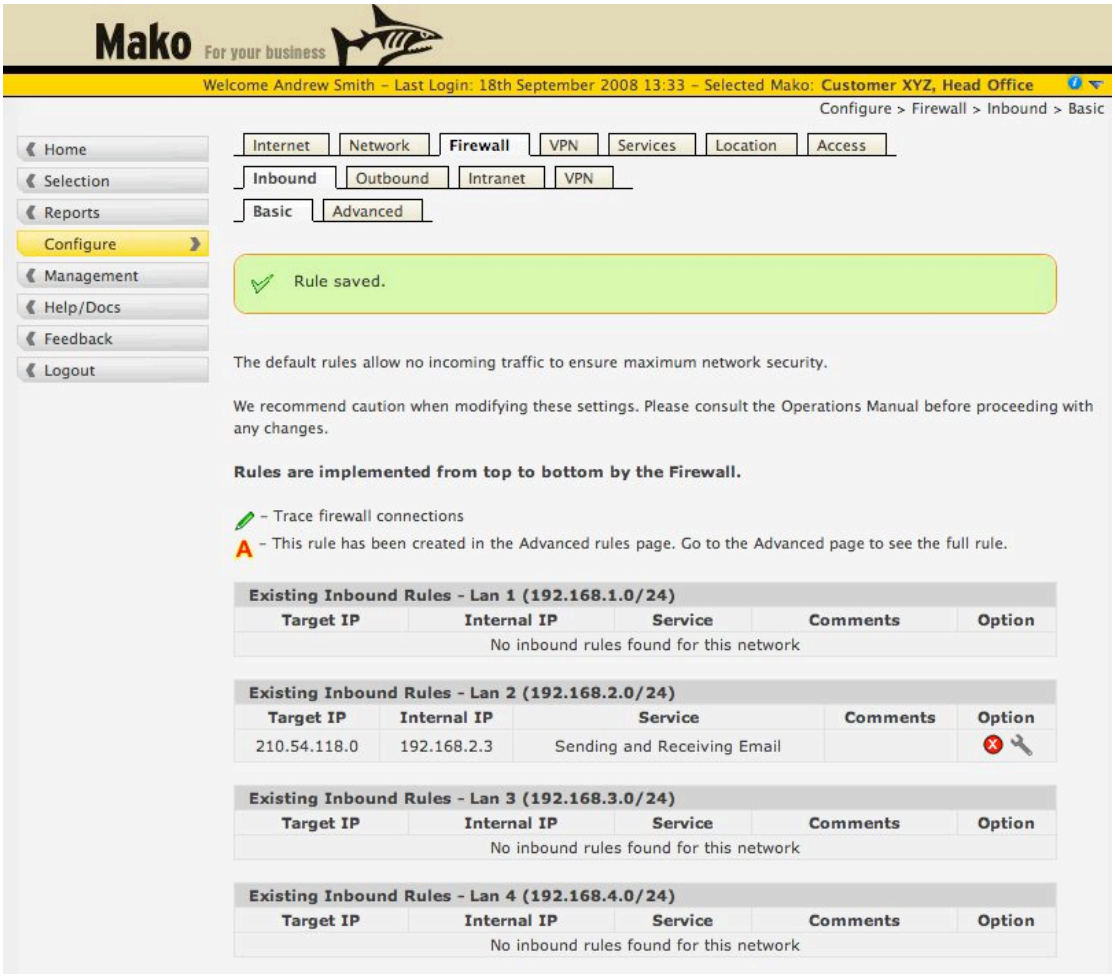
Firewall, Basic Inbound

The access path is referred to as a 'Pinhole' through the firewall. A Pinhole is an access path which is as restricted as possible. In this case it specifies the mail server as the sole target, and the email protocol as the sole communications protocol. Since any mail server may have email for the office it is not possible to specify the IP address of the host which initiates the communication.

The Basic screen above provides the simplest approach to creating a Pinhole. The Add Pinhole table permits the selection of a specified protocol from the drop down menu to be connected to a specified local (internal) IP address.

If you are unsure of what local IP address you should use you can click on the [lookup] link which will show you all PCs the Mako is aware of behind it.

Once you have added a rule you can edit it by clicking on the Spanner icon.



Firewall, Basic Inbound with Mail Pinhole

Enter the target machine's IP address, the Service protocol which is allowed to access that machine, and click on Add to enable the Pinhole. Pinholes can be removed by clicking the corresponding Delete button in the upper table.

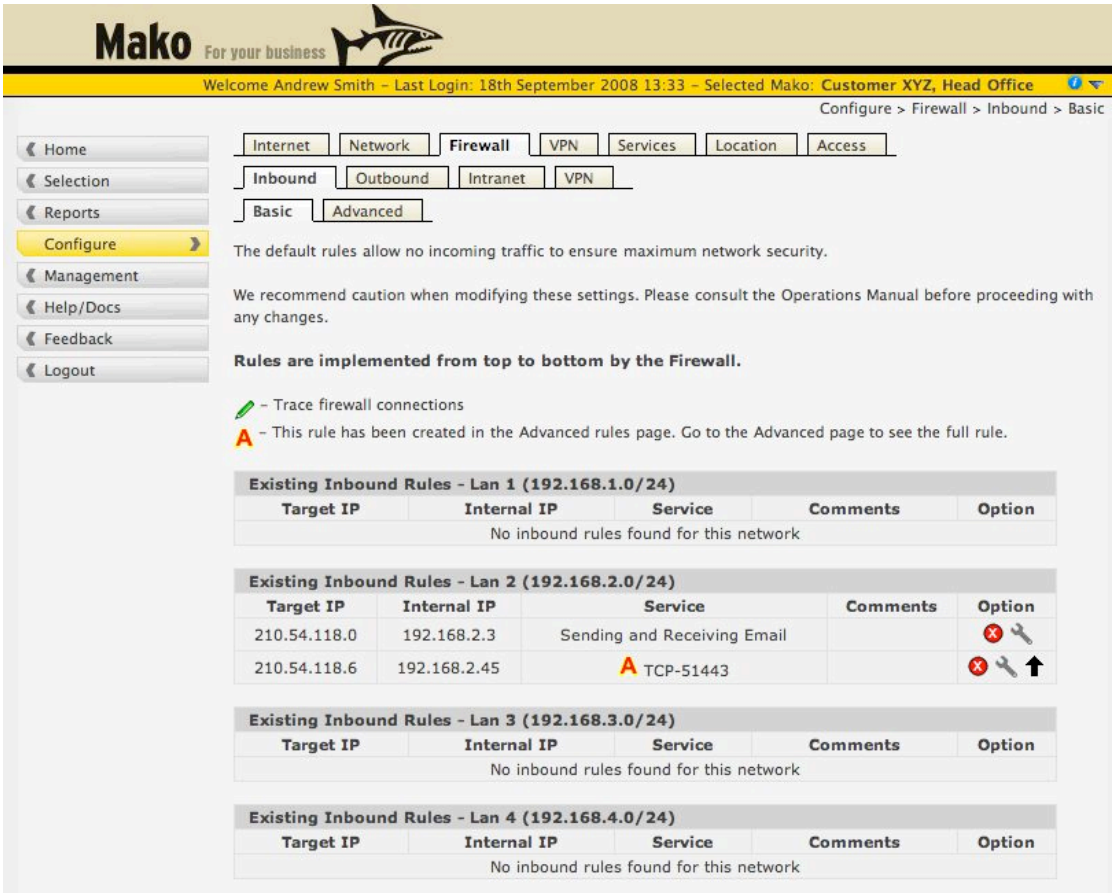
If your ISP provides you with multiple public IP addresses you may specify a public IP address that the inbound pinhole refers to. This is useful if you want to have multiple pinholes to the same port on different internal PCs.

The Comments field is optional and provides you with a space to enter reminder details about the rule/pinhole.

Considerations
The Internal IP Address has to be static, that is, not able to be re-assigned by DHCP. Please refer to the previous section for details.

The Service defines exactly which Internet protocol is permitted to communicate through the Pinhole. A wide choice of the most frequently found protocols is available from the drop down menu under Service. Where an additional protocol is required simply email the address shown and it will be added to the list.

More complex firewall configurations are covered in the next section. An example of the Basic screen when rules have been configured in the Advanced section appears below.



Basic Inbound Firewall Rules

Here one of the rules operating on the firewall is shown as having been created on the Advanced rules page.

Inbound: Advanced
This section allows more complex access permission rules to be configured than those available on the Basic screen in the previous section. Please review the discussion in the previous section for background information on the issues involved.

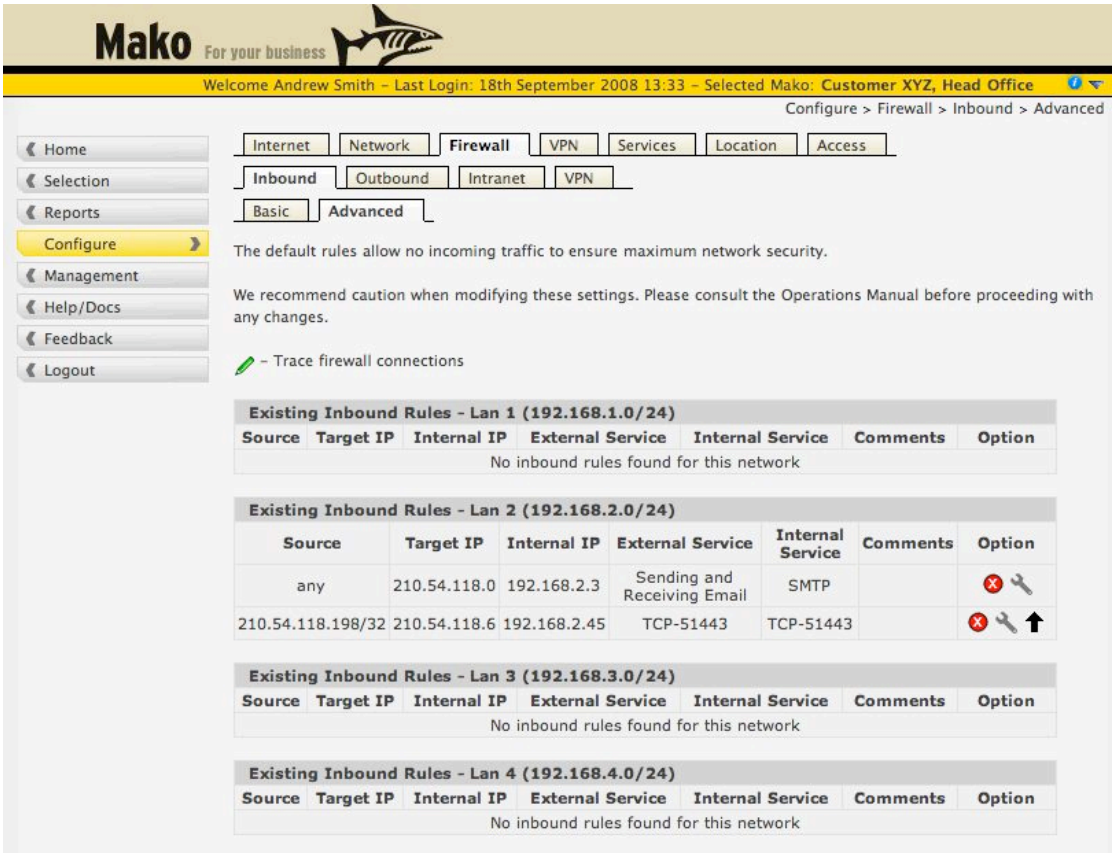
Similar principles apply in terms of defining Pinholes which are as restricted as possible.

Permission rules are defined covering the Source (or External) IP address, the Destination (or Internal) IP address, the External Service and the Internal Service.

Thus it is possible to specify the Internet address of the machine which is initiating communications and the protocol which that machine may use in its communications, as well as those of the machine on the office network.

To add a new Pinhole, enter the IP addresses and their corresponding Services in the lower table and click on Add. To remove a Pinhole click on the corresponding Delete button.

The screen shot below is an example of Advanced rules configuration. The screen shows the rule flagged as Advanced on the Basic configuration page, earlier.



Advanced Inbound Firewall Rules

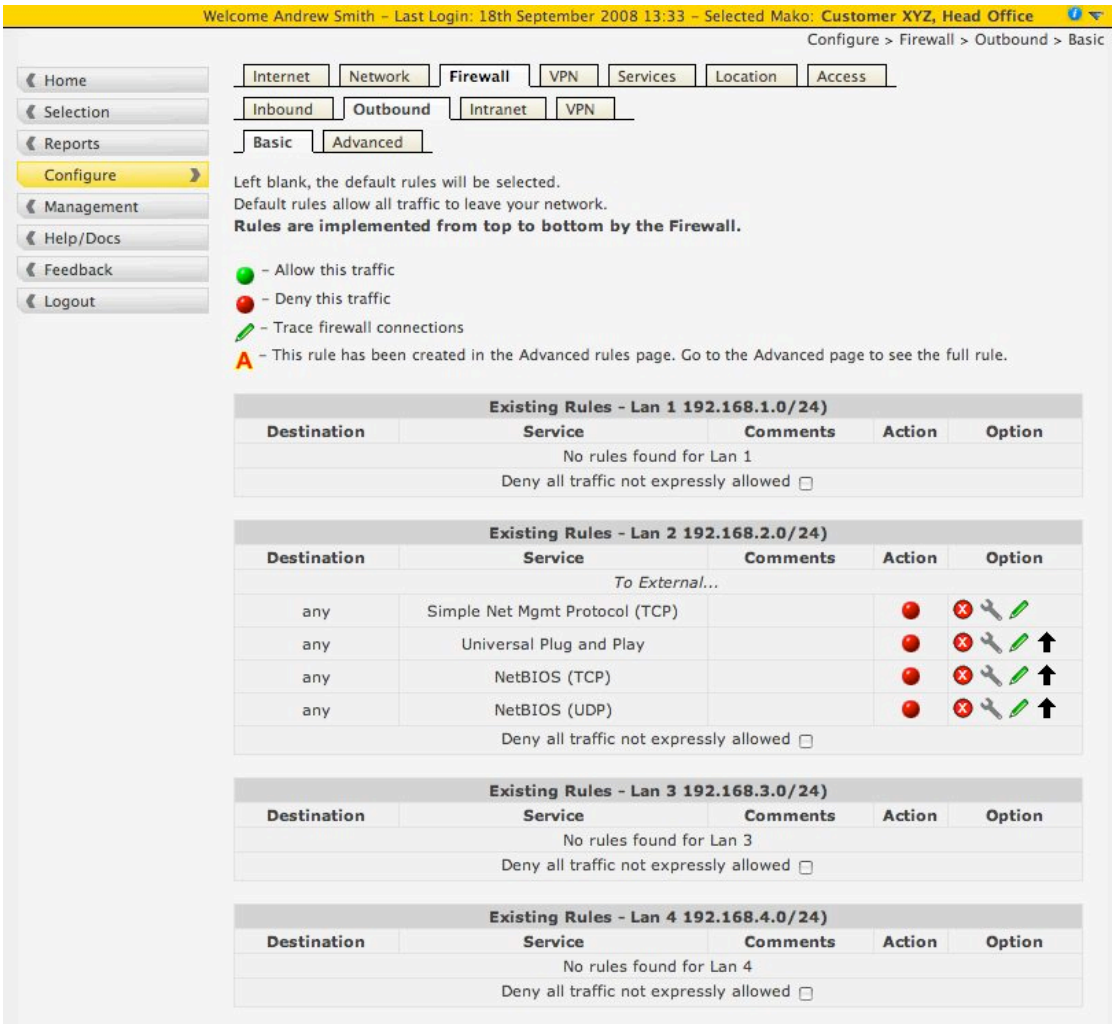
Note that the option of declaring IP addresses as “any” has been selected, to allow any Internet based host to open communications with the target local computers. This is achieved by leaving the Source IP Address/Mask fields empty.

If your ISP does not provide you with multiple public IP addresses you will not see the Target IP Address drop-down.

You may specify a public IP address that the inbound pinhole refers to. This is useful if you want to have multiple pinholes to the same port on different internal PCs.

You may specify to log debugging information when a connection through an inbound rule is attempted. The Trace Logging checkbox, when checked, records the debugging information which is then made available to your Reseller in the Syslogs Report section of the website. The Trace Logging option is also available in the Outbound Advanced and Intranet Advanced sections.

Outbound: Basic
By default, Outbound traffic is not filtered. Please review the discussion earlier in the Firewall section for background information on the issues involved.



Firewall Rules, Basic Outbound

The screen shows how any given rule can be set up to Deny or to Allow the specified traffic.

In this example three protocols which may pose security issues for an Internet connection are prevented from passing from any internal machine on Lan 2 out through the firewall.

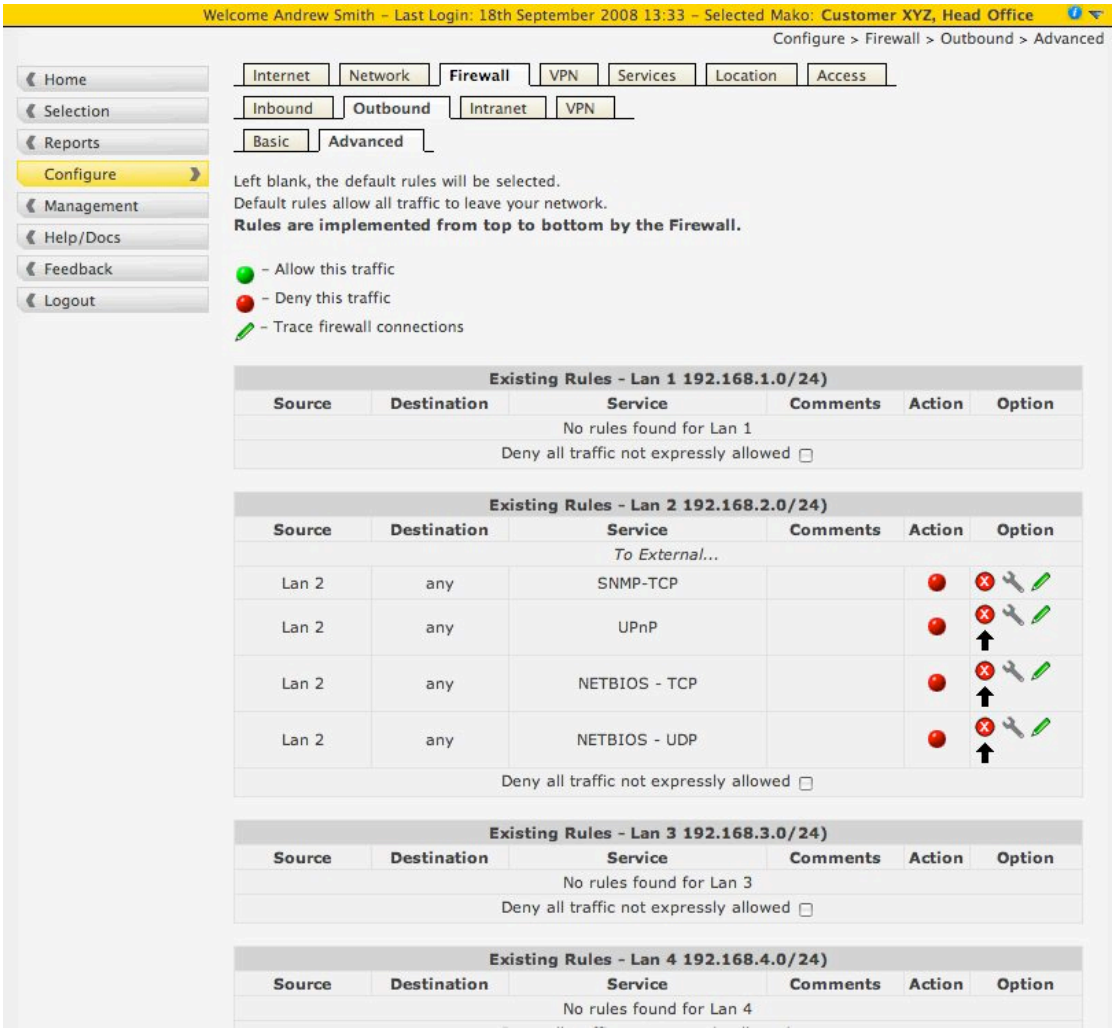
There is also the option of Denying all traffic not expressly allowed. This is a convenient way to set up your rule structure, as it means that once the box is checked, only required access permissions need be addressed. These can be set up as Allowed. All others are blocked.

To ensure that a rule to permit Allowed traffic does not inadvertently open unwanted access by subverting the operation of another rule, rules are applied in sequence. This establishes a hierarchy in the application of rules.

Once you have added a rule you can edit it by clicking on the Spanner icon.

Outbound: Advanced

As with Inbound Security, the Advanced screen permits more complex permissions to be set up. Please review the discussion at the beginning of the Firewall section for background information on the issues involved.

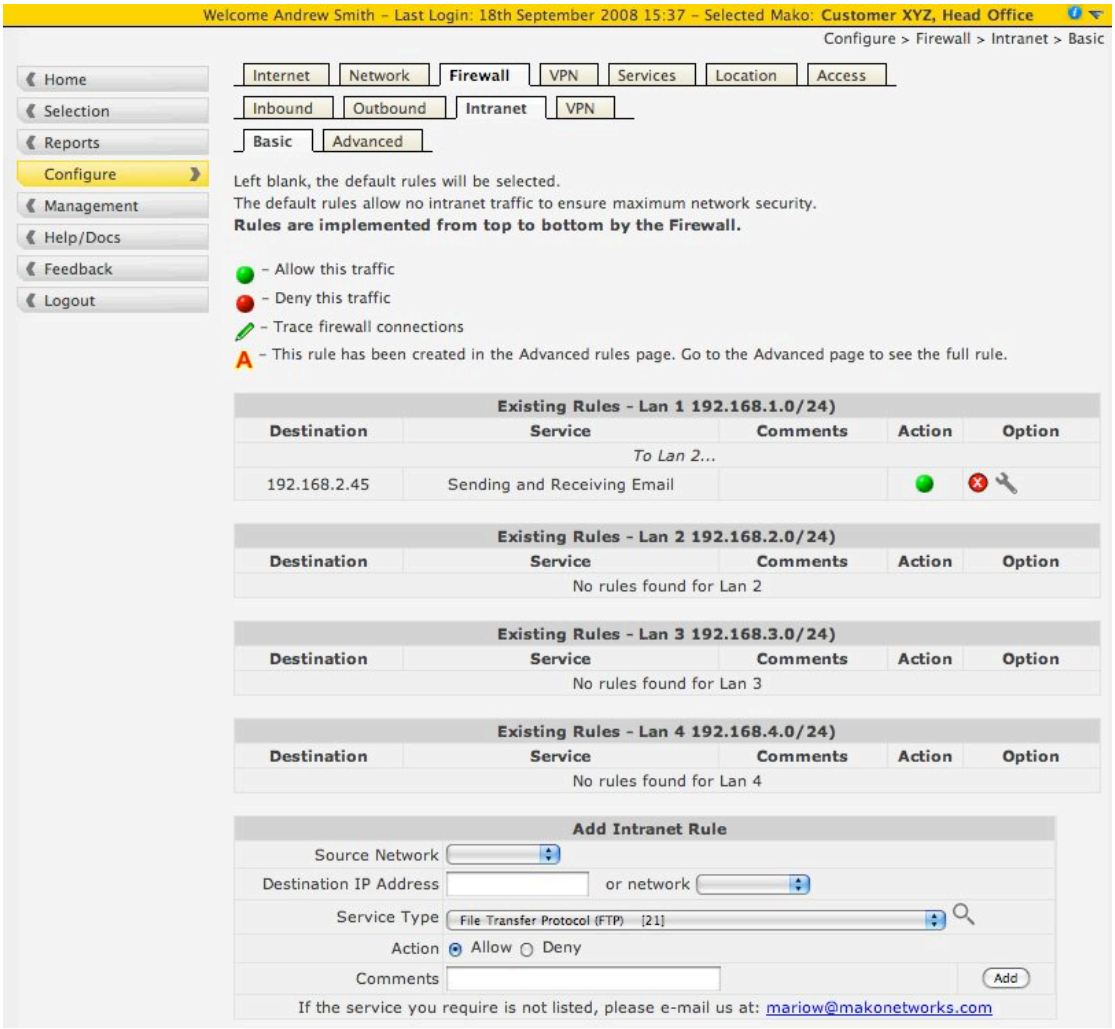


Firewall, Advanced Outbound

The screen shows an example of rules set up to prevent unwanted traffic from being passed out through the firewall.

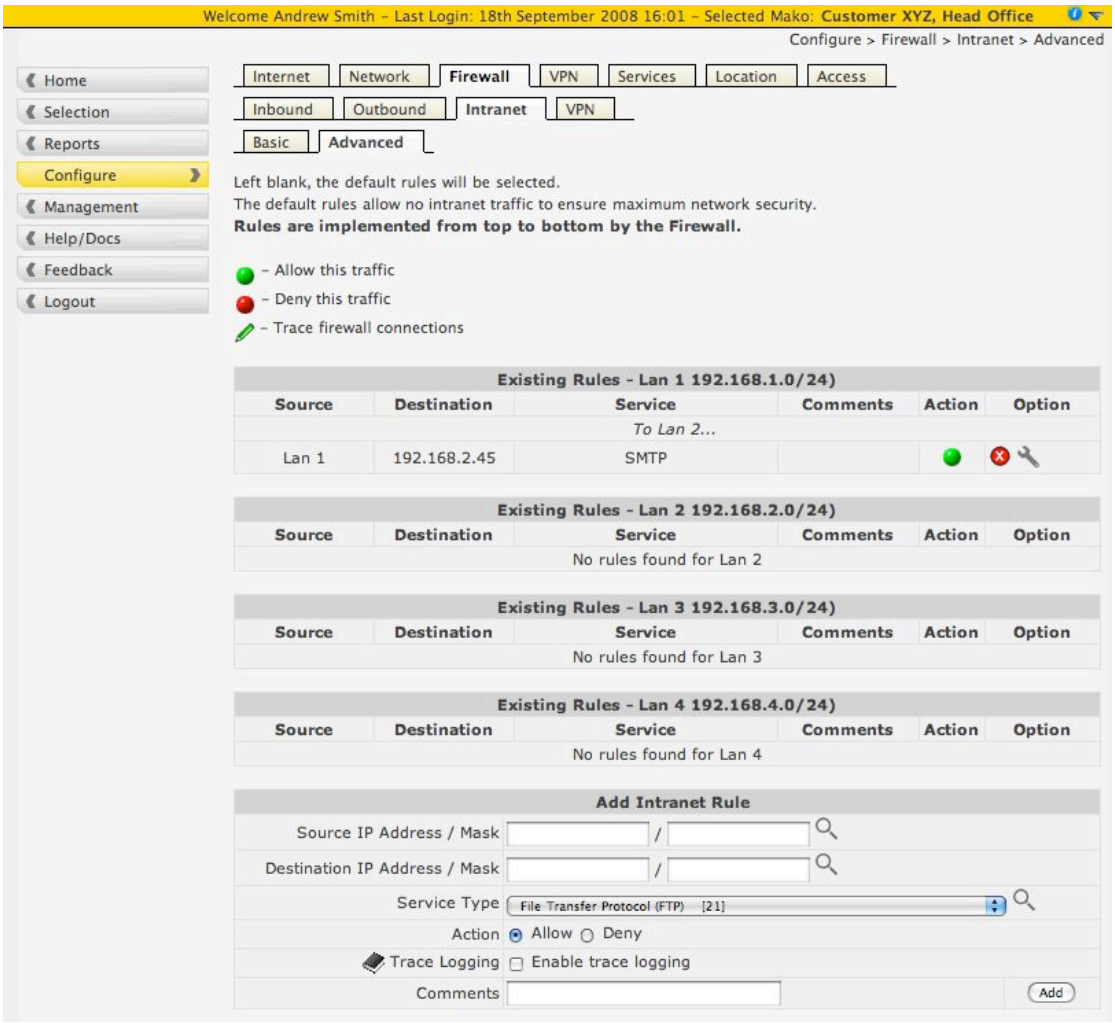
Intranet: Basic

The Intranet Firewall rules allow you to allow or deny traffic between your four Mako 7550 protected networks. It is not normally recommended to change from the default settings as you could reduce the security provided by separating the networks.



Firewall, Basic Intranet

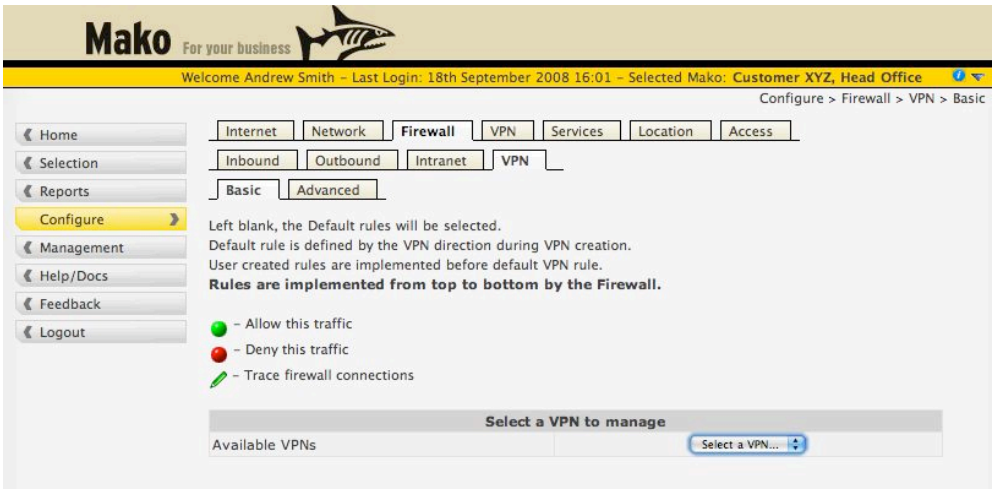
Intranet: Advanced
As with Outbound Security, the Advanced screen permits more complex permissions to be set up.



Firewall, Advanced Intranet

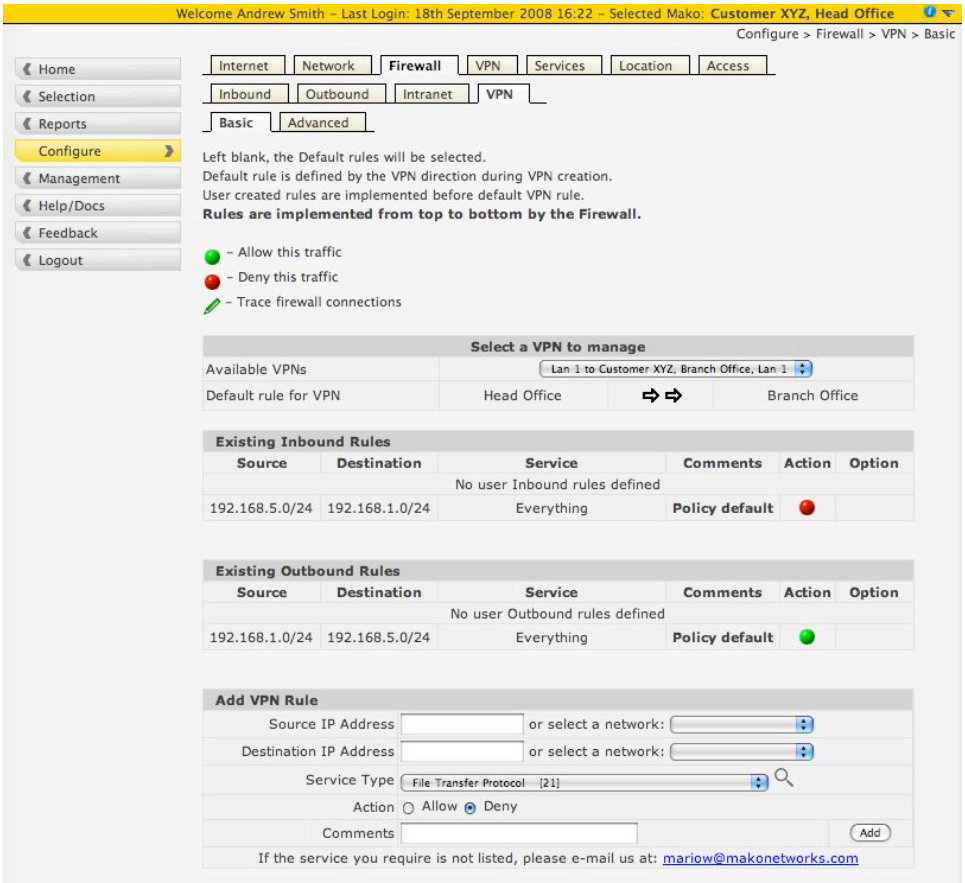
VPN

VPN Firewalling enables you to control the flow of data across Mako to Mako VPNs and Third Party VPNs. Normally, once a VPN is created the traffic flows freely from network to network. If you want to restrict access to the VPN to specified computers or to a certain type of traffic, VPN Firewalling is the answer.



VPN Firewall

Control of the traffic uses a similar interface to inbound and outbound firewall controls. First you must select your Mako to Mako VPN from the drop down list of Available VPNs. Once you select which VPN you are wanting to Firewall, the screen changes to give you control as depicted below. The method for adding rules is the same as for Inbound and Outbound except that the Default rule for VPN remains at the bottom to remind you the basic setup of the tunnel.

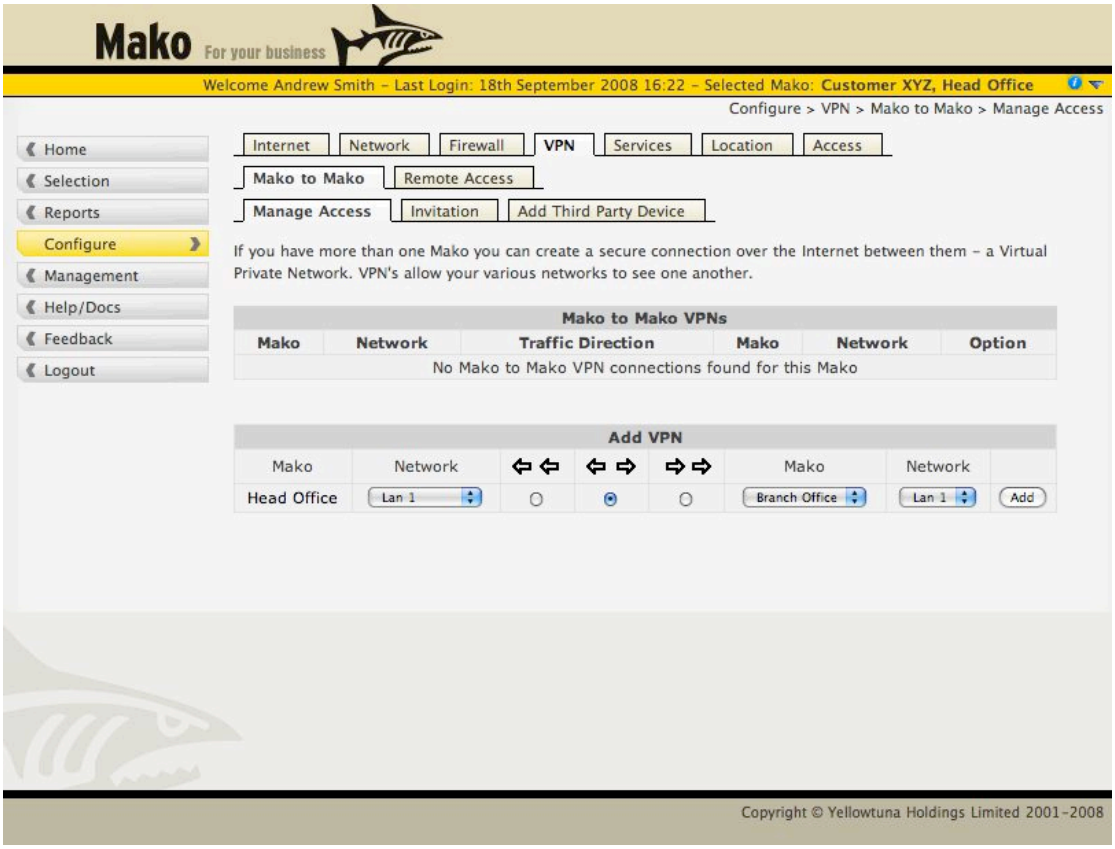


Firewalling a VPN

Configure: VPN

Mako devices have two types of VPNs available, Mako to Mako and Remote Access.

Mako to Mako
If you have two or more Mako units, this screen allows you to set up secure virtual private network communications between each pair of Mako protected networks.



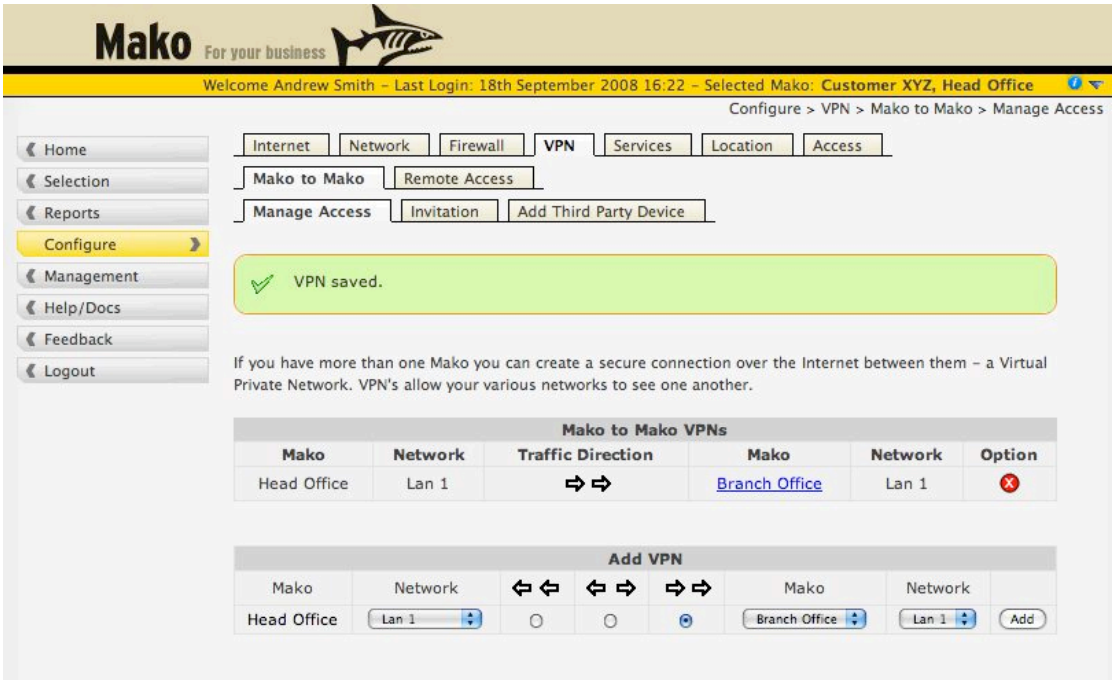
Mako to Mako VPN Screen

There are two steps to set up a VPN link:

1. First use the drop down menu as shown to select the other Mako appliance you wish to configure as the other end of the VPN link. If either Mako is a 6086 or 7550-type Mako, select which protected network you want to link.

2. Now decide access rights over the VPN link. You can choose between three visibility options. Either the computers locally connected to the Selected Mako can see those at the other Mako device, but not the reverse; or the other way around; or both ends can see the computers on each others network. Click on the button under the arrows showing the required direction of visibility.

Click on Add to save the VPN configuration. It will now show up in the table, as shown in the example below.



Mako to Mako VPN

This shows VPN access set up so that computers on Lan 1 at Head Office can see those on Lan 1 at Branch Office, but those at Branch Office cannot see the ones at Head Office.

Considerations
It is important to ensure that the local private network IP address scheme behind the Mako devices at each location is different. This will occur if you leave the Mako appliances at their default address as supplied from your Reseller.

For example, the London, LAN 1 may use the address range: 192.168.1.xxx, while Head Office, LAN 1 would be 192.168.3.xxx (where xxx is the range of addresses used at each network). The significant element is the highlighted '192.168.1.' and '192.168.3.' — these must be different at the two ends of the VPN link. Please contact your Reseller if you have any questions regarding the best choice of private IP addressing schemas for your offices.

The corresponding changes to the secure profile of the Mako unit at the other end of the VPN link will be made automatically. It is not necessary to update both configurations.

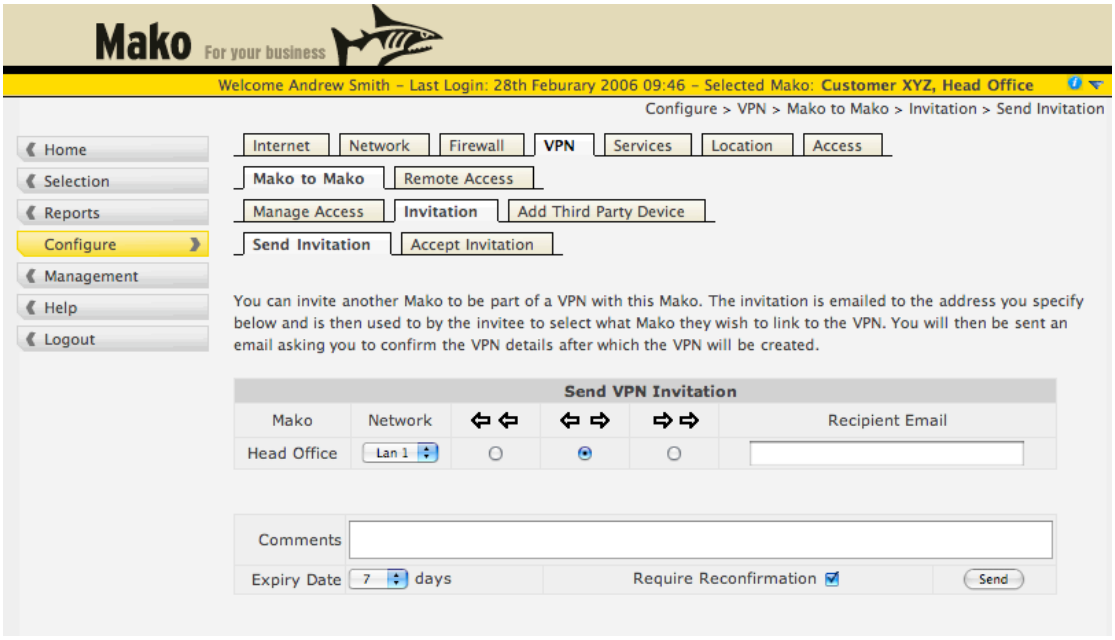
This makes it straight forward to set up a temporary secure link between your Mako devices and then remove it when the requirement ceases.

The update will take about 2 minutes to propagate out to the Mako devices, or they can be power cycled for the update to be initiated straight away.

Invitation
If you wish to have a Mako to Mako VPN between your Mako and a Mako that belongs to another company, you can do so with Mako VPN Invitations.

Invitation: Send Invitation
To create a VPN between a Mako you can administer and one you cannot, you need to know the email address of the administrator of the other Mako.

The Mako you have currently selected will appear in the bottom left hand side of the Mako Send Invitation page. Select which LAN you want to be your part of the VPN, select the direction of the VPN in the same manner as Mako to Mako VPNs and enter the email address of the administrator of the Mako you are wanting to connect to.



VPN, Mako to Mako, Invitation, Send Invitiation

The administrator of the other Mako will receive an email with a special key inviting them to accept your invitation and create a Mako to Mako VPN with your Mako. If you like you can add comments that will be added to the email. By default, the invitation will be valid for seven days. After this time the key will not work and you will have to begin the invitation process again. You can change the length of validity of the invitation by changing the Expiry Date.

The Require Confirmation box will also be checked by default. This is to add an extra layer of security to the invitation process. With this box checked, after your invitation has been accepted, you will receive a confirmation email with another key in it that you will need to accept before the VPN is established. If you remove the check from Require Reconfirmation, this process is skipped and the VPN is established once the invited party accepts.

Invitation: Accept Invitation
Once you have received a Mako to Mako VPN Invitation by email, you need to go to the Accept Invitation screen and enter your key.

VPN, Mako to Mako, Invitation, Accept Invitation

Simply copy the key and click continue. If the Require Reconfirmation box was checked by the invitation initiator then the initiator will need to complete this process. If the Require Reconfirmation box was unchecked then the VPN will be established.

Once the VPN is established it will appear in the Mako to Mako VPN Manage Access list. Either party may delete the VPN at any time.

Third Party VPN
If you use a non-Mako router to connect to the Internet at a remote site, you can create a VPN connection between your Mako and the third-party device.

The third-party device must support:

- IPSec VPN's
- 3DES IPSec Encryption Algorhythm
- MD5 Authentication Algorhythm
- Diffie-Hillman 1024 Public Key Algorhythm
- Support for Pre-Shared Keys

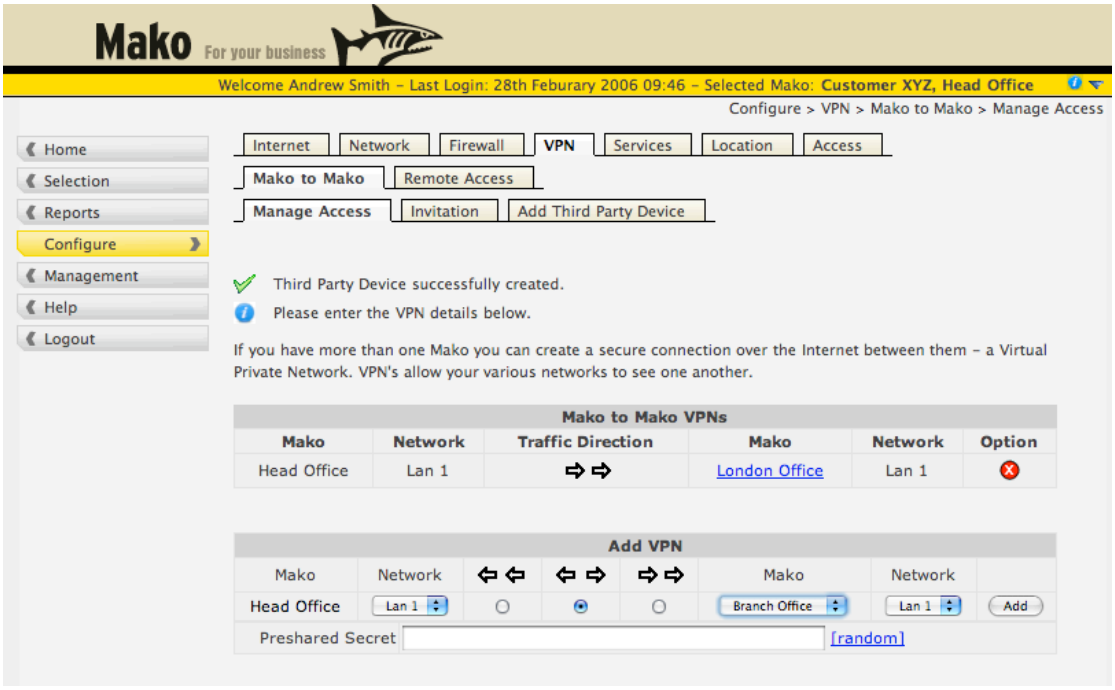
In addition both the Mako and the third-party device should have static public IP Addresses in order that the VPN be kept alive for any length of time.

To configure the Mako to be able to connect to a third-party device click on the Add Third Party Device sub-menu.

Add Third Party Device

Type in the location of your non-Mako router, enter its public IP Address and provide the network details of the LAN behind it. Then click Add and Create VPN. This will take you back to the Mako to Mako VPN page.

The third-party device will appear at the bottom of the right-hand Mako list. Select that device and you will see a screen like the one over page.



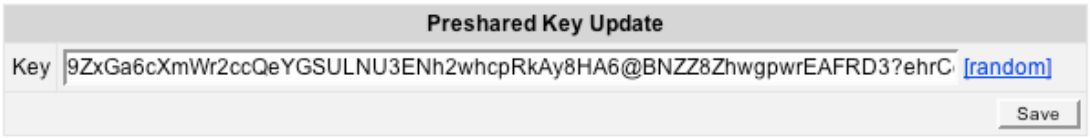
Third Party VPN setup

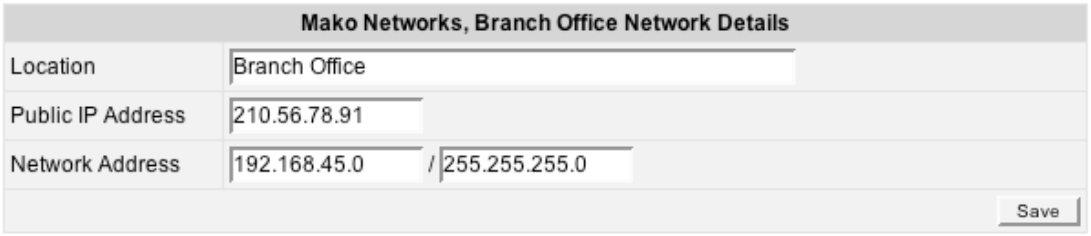
You can now either enter a Pre-Shared Key or create one automatically by clicking the [random] link. Then click Add. The Mako will then be awaiting the third-party device to form the connection.

Mako	Network	Traffic Direction	Third Party	Network	Action
Head Office	Lan 1	⇦ ⇨	Branch Office	Lan 1	

Third Party VPN Established

You can modify any of the settings of an established Third Party VPN by clicking on the Spanner icon.





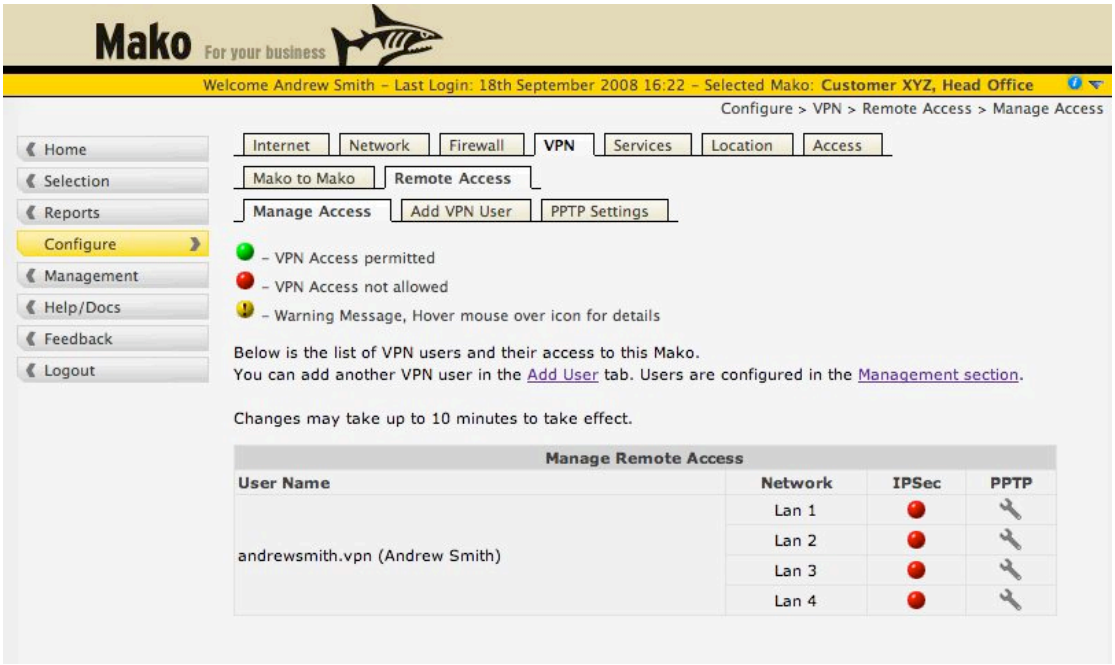
Third Party VPN Modification Screen

Remote Access
Mako Networks offers two types of Remote VPN connection – IPSec and PPTP. IPSec is more complicated to setup and generally requires additional software on the client but is very secure. PPTP is easier to setup and most Operating Systems support PPTP natively but it is less secure than an IPSec VPN.

Please see separate Documentation on client setup for each type of Remote Access VPN.

In the interests of security, you must create VPN-Only usersname and password combinations in the Add Users section in order to access Remote VPNs. Usernames and Passwords that are already used to access the Mako Networks website cannot access Remote VPNs.

Any user recorded in the subsequent Add User section can have their network access enabled and disabled as appropriate. For best security it is highly desirable that they are permitted access only while they need to use the office network — at other times their access should be disabled.



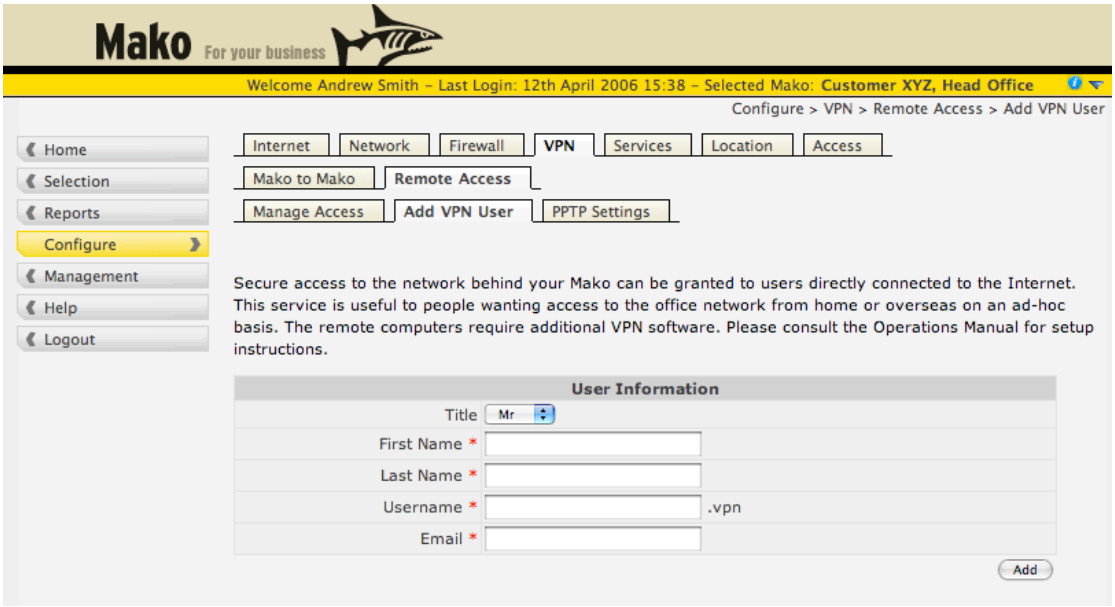
VPN, Remote Access

When the indicator for a particular type of VPN is red, that VPN type is disabled for that user. To enable, click the red indicator and it will change to green. Disabling is done in the reverse manner.

Considerations
There are two areas which affect the remote VPN user. First is the way in which they connect to the Internet. Second is the software package they must use to provide a secure wrapping for their communications, while connected to the office network.

Connection Method
See the documentation section of the Mako Networks website for details on how to Remote VPN using specific IPSec or PPTP VPN Client software.

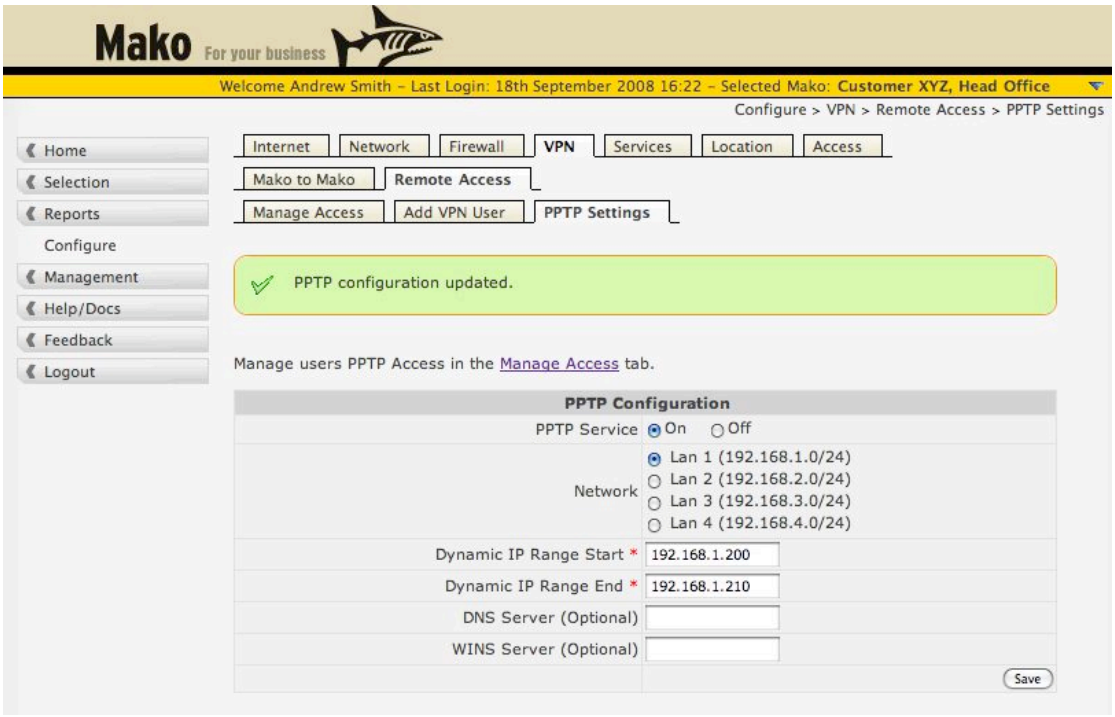
Add Users
This screen allows you to record details of a user for administrative purposes. The 'User Name' field gives you a convenient nickname for quick identification.



Remote VPN, Add User

As each user is recorded, click on Add to save the information. Usernames will automatically have the .vpn extension appended to identify then as a VPN user and not an administration user. Once a user is recorded their access can be individually enabled or disabled at any time, as shown in the previous section.

PPTP Settings
PPTP is not enabled by default. This is because enabling PPTP brings with it some risk. To enable PPTP, click the On radio button.



PPTP Settings

Choose which LAN network you wish to enable PPTP access to. You can only enable PPTP access to one LAN.

You then must set a range of LAN IP Addresses that will be issued to PPTP VPN users when they connect to the Mako and have the option of issuing an internal DNS Server and WINS Server IP to the PPTP VPN users.

When you have finished setting this up, click the Save button. You can now enable each user you wish to have PPTP access from the Manage Access screen.

Configure: Services

Mako 7550 devices can have many optional services added. Please check www.makonetworks.com for the latest available services.

Documentation for Services that carry an additional cost can be downloaded in PDF format from the Documentation section of the Mako Networks website. If you would like this documentation emailed to you, please send an email to support@makonetworks.com.

QoS
QoS stands for Quality of Service. QoS comes standard with 7550 series Makos. This feature allows you to prioritise different types of Internet traffic and specify minimum outbound bandwidth allocations. QoS can be used to improve the quality of such services as Voice over IP traffic by ensuring there is always bandwidth reserved for it.

On the Internet, QoS is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance.

QoS: Basic
The Mako default setting is recommended for most users. This setting allocates bandwidth reservations to the most common Internet applications and traffic types.

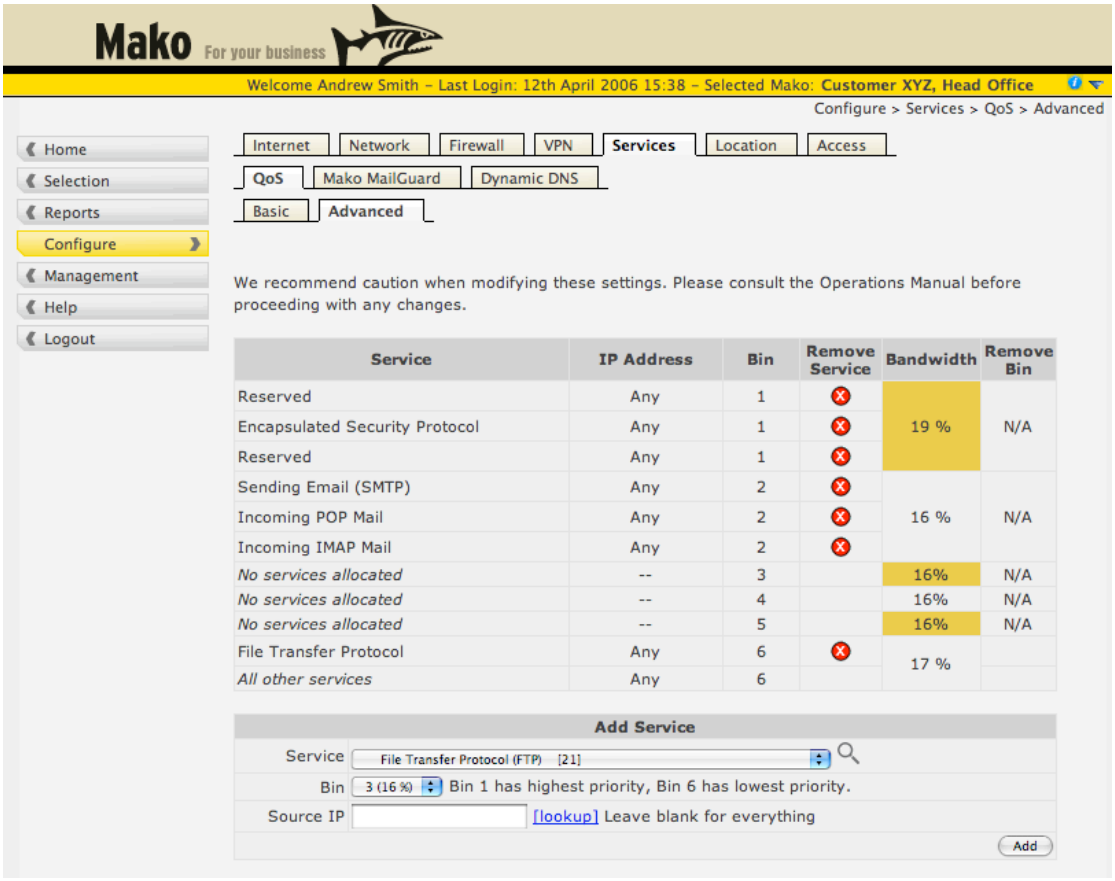
Quality of Service, Basic

The VoIP Enhanced setting guarantees VoIP traffic approximately 33% of your upstream bandwidth. Use this setting if you require enhanced VoIP quality and reliability.

QoS: Advanced
The QoS Advanced section is recommended for experienced users only. Please consult your IT Provider if you have any uncertainty about these settings.

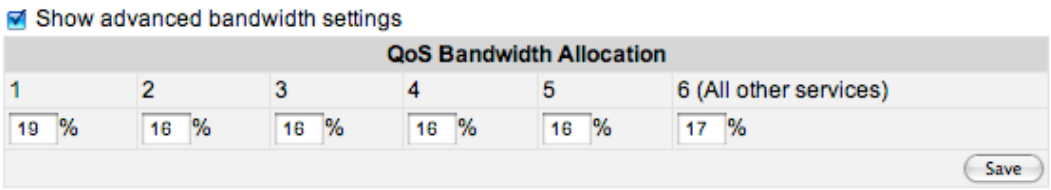
The upstream bandwidth is broken into 6 “Bins”. Bin 1 has higher priority than Bin 2 and Bin 2 has higher priority than Bin 3 and so on. You can group various Internet Services into different Bins. All services that belong to a particular bin share its bandwidth. Important or high priority services should be placed in a bin with no more than 2 other services to ensure the bandwidth for the bin is not shared between too many services. All the services in a Bin share that Bins allocation of bandwidth. The services are guaranteed that Bins percentage of bandwidth as a minimum. If some upstream bandwidth is unused, it can be temporarily borrowed from other bins until the bin needs the bandwidth.

Services that are not allocated to a bin use the last bin by default.



Quality of Service, Basic

By placing a tick in the Show advanced bandwidth settings box you can allocate upstream bandwidth percentages across the Bins.



Advanced QoS Bandwidth Settings

Dynamic DNS

All Mako devices support Dynamic DNS. Dynamic DNS requires a free subscription to one of two third-party Dynamic DNS providers – DynDNS.org or no-ip.com

Mako Networks neither endorses or in any way guarantees the services provided by either of these parties. The Dynamic DNS service provided by Mako Networks is provided as a convenience to the users of its products and Mako Networks has no control over any aspect of DynDNS.org or no-ip.com.

A Dynamic DNS service allows you to have a fixed address on the Internet without the need for a static IP address. Once you have an account with either of our two support Dynamic DNS providers, they will give you a domain name. The Mako will then update the provider with its current public IP address so the domain name references the correct address. This way the domain name remains static and has the IP address it references updated automatically by the Mako System.

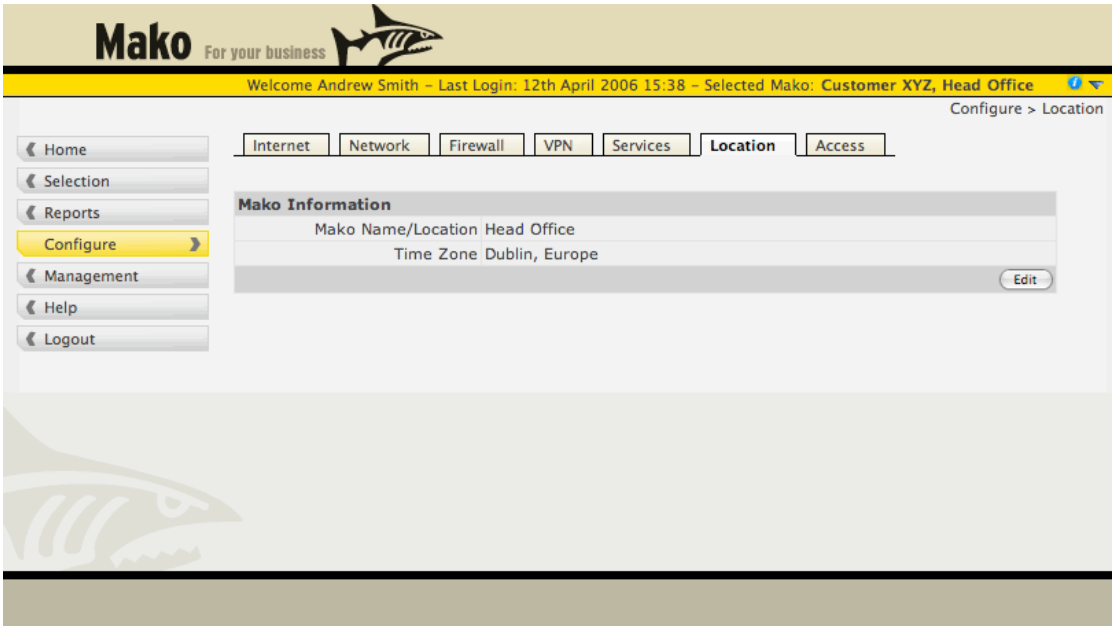
To sign up to one of these services, follow the instructions and documentation on the providers website. You will receive a Username and Password from your Dynamic DNS provider. Enter this information in the appropriate section on the Mako Networks Dynamic DNS screen. Once entered, each time your Mako changes public IP address, it will update your Dynamic DNS provider.

Dynamic DNS No-ip configuration

Configure: Location

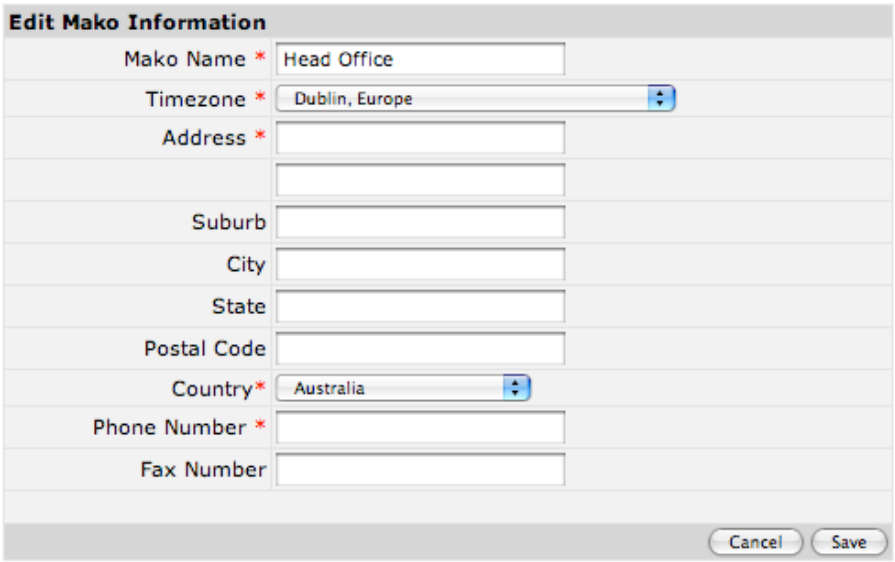
The Location section allows you to update and view the non-technical details of your Mako device.

Mako Information
This screen allows you to review or update information relating to the physical location of your Mako.



Location

By clicking the edit button you can add additional location information.



Add Information

Configure: Access

From this screen you can view which users have access to this Mako. You can change access rights to Resticted Users.

Access Control

Management: Home

This is the home of the Management section. Wheras the rest of the site is for administering Mako end points, the Management section is for administering Users and Company information.

By default, your own User and Company are selected and shown in the top right of the screen under the Shark logo.

Company and User selection

Management: Company

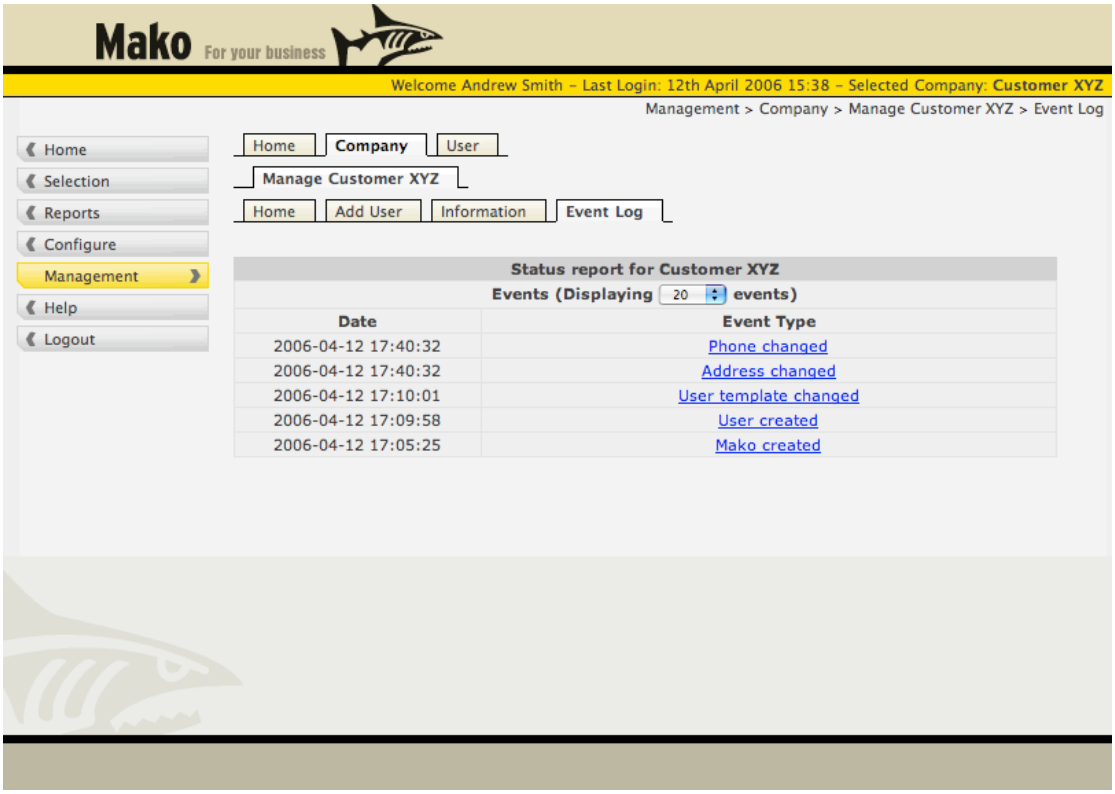
In this area you can administer your Company(ies) information.

Add User
This button links you through to the Management: Users: Add User screen described later in this document.

Information
This is where you store Company related contact information. This is separate from Mako contact information.

Company Information

Event Log
A log of changes that have been made to your Company is available here.

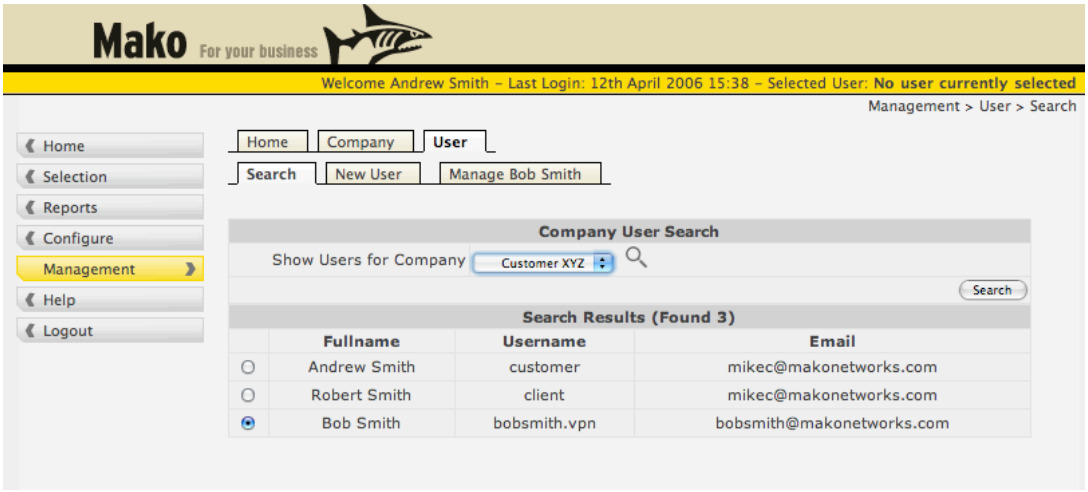


Event Log

Management: User

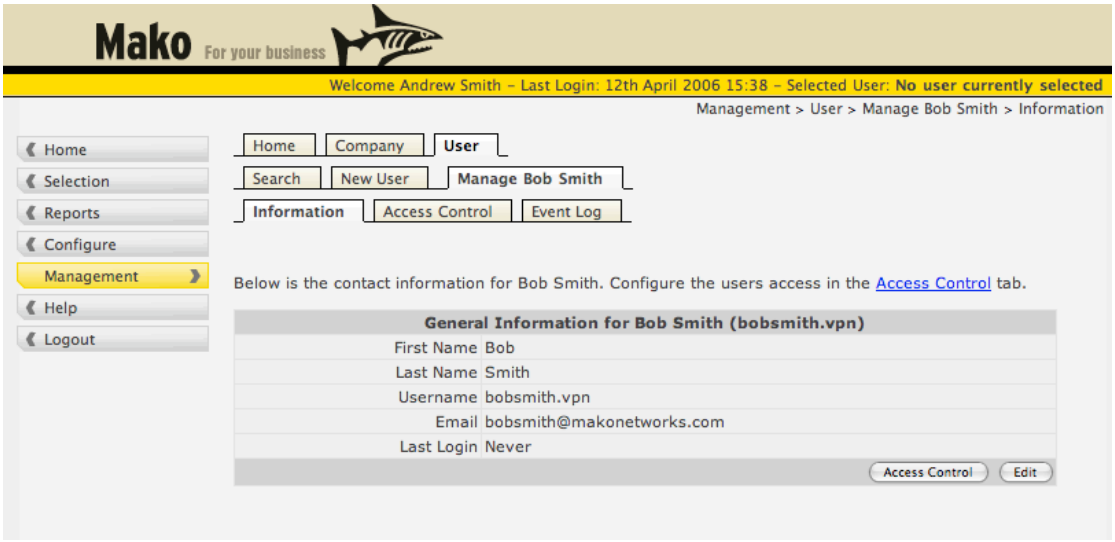
From here you can add, modify or delete users within your company. When creating or modifying Users, you can grant permissions that are equal to or less than your own rights.

Search
This is the default screen when you click on the User tab. It lists all the Users for your Company or lets you choose which Company's Users you want to view if you have more than one Company.



User Search

Once you select a User, you will either be taken directly to the Manage User screen or you will be able to click on the Manage User submenu depending upon which browser you are using.



Manage User

From the Manage User screen you can view the contact information for the User and edit it by clicking the Edit button as shown below.

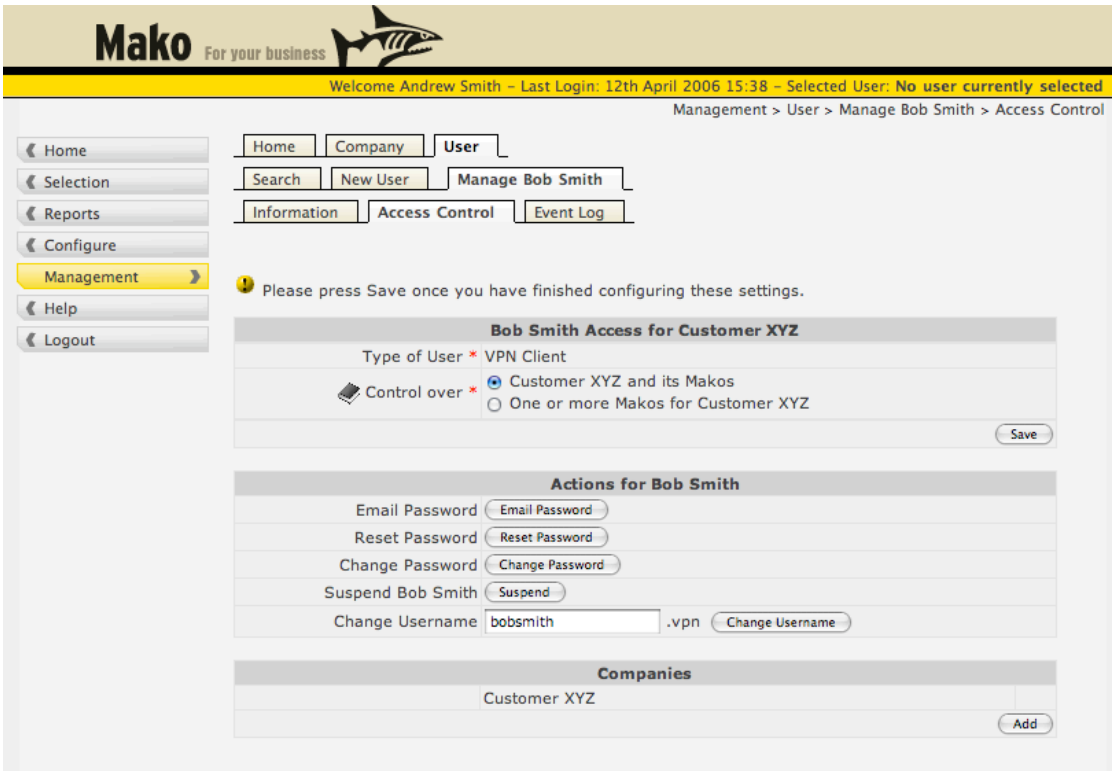
Edit User

Once you have edited the Users details, click save and the main page will refresh to reflect your newly entered details.

From the Manage User Information screen you can also edit the Users access by clicking on the Access Control button.

This will take you to the Manage User, Access Control submenu.

You cannot change your own Access level, only the Users you have created. You may only grant other Users Access equal to or less than your own access.



Access Control

You can change the Type of User. In this example, the User Thomas Smith is a Basic Client and only able to view reports. You could change him to a Full Client which will enable him to configure Makos.

The Control over section allows you to either have contol over all of your Company's Makos or just a selected group.

From this screen you can also Email the User their password if they have forgotten it, Reset the Password which will generate a new password and email it to the User or Suspend the User which makes them unable to log into the system. This is useful for contractors or occasional Users.

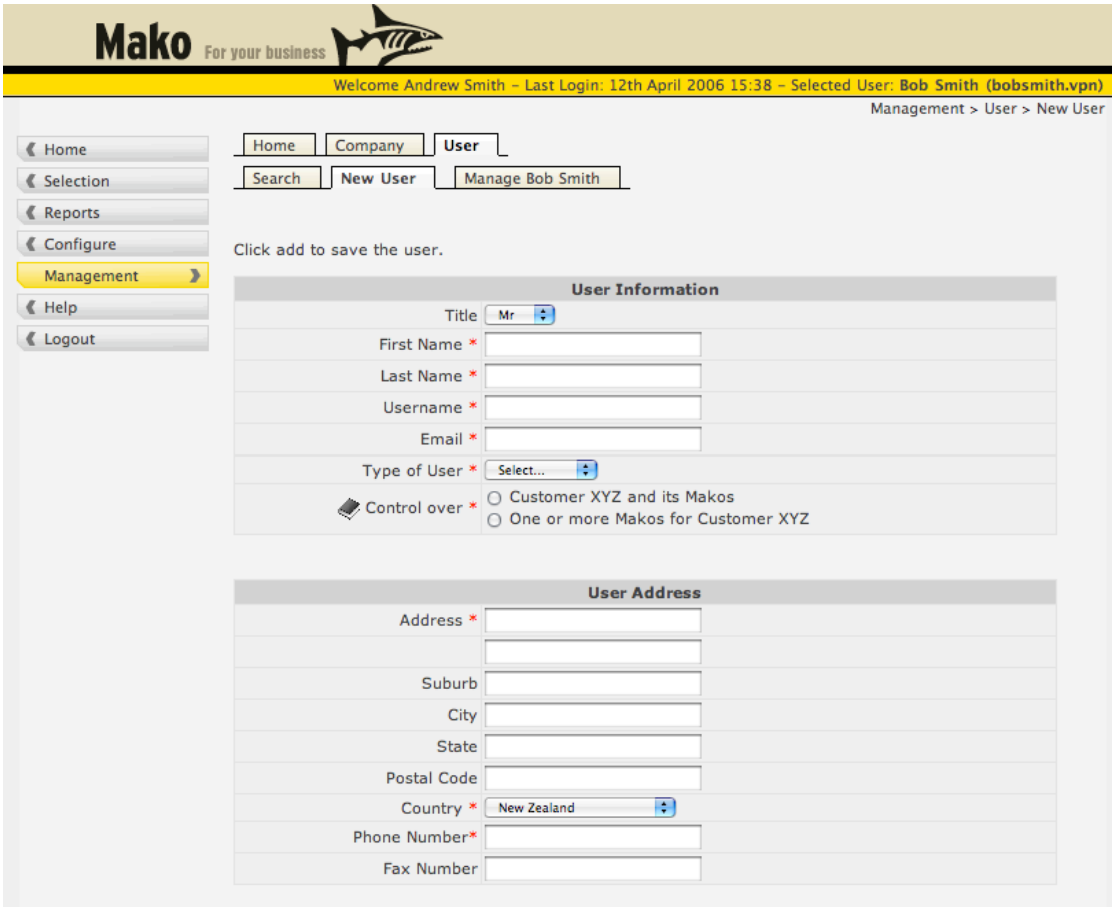
If you wish to change the Username the User has to log into the system, you may also action this from this page.

Event Log

The Event Log is a history of all recent changes that have been made to the selected User.

User Event Log

New User
From here you can add a new User to your Company and grant them access to all or some of your Company's Makos.



New User

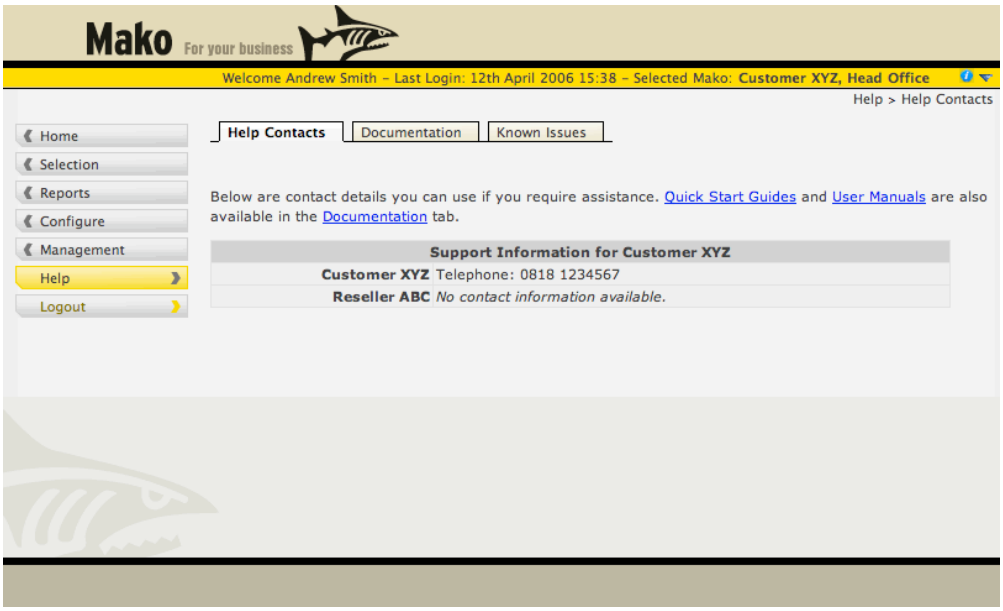
Fill in at least the fields marked with a red asterisk. It is important that you correctly enter the Users email address as the randomly generated password will be sent to that email address.

You can choose the type of user to create and whether you want to grant access to all your Company's Makos or just some.

When you have completed this information, click the Add button at the bottom of the page.

Help: Help Contacts

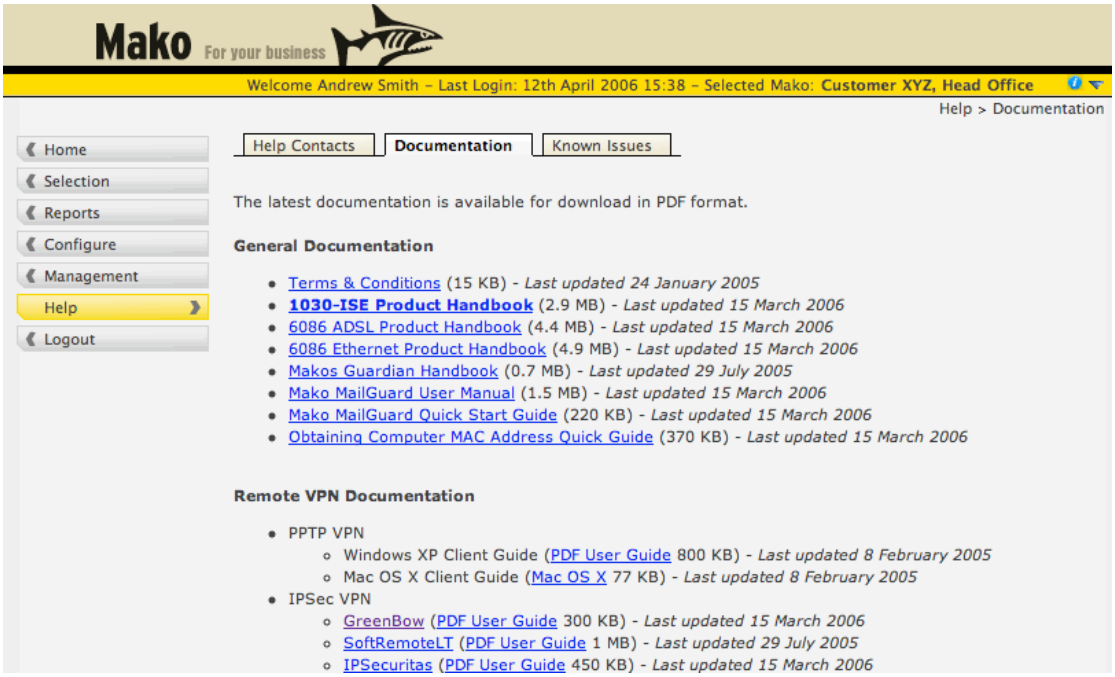
This screen contains the technical contact details for your company and its IT Provider(s).



Help Contacts

Help: Documentation

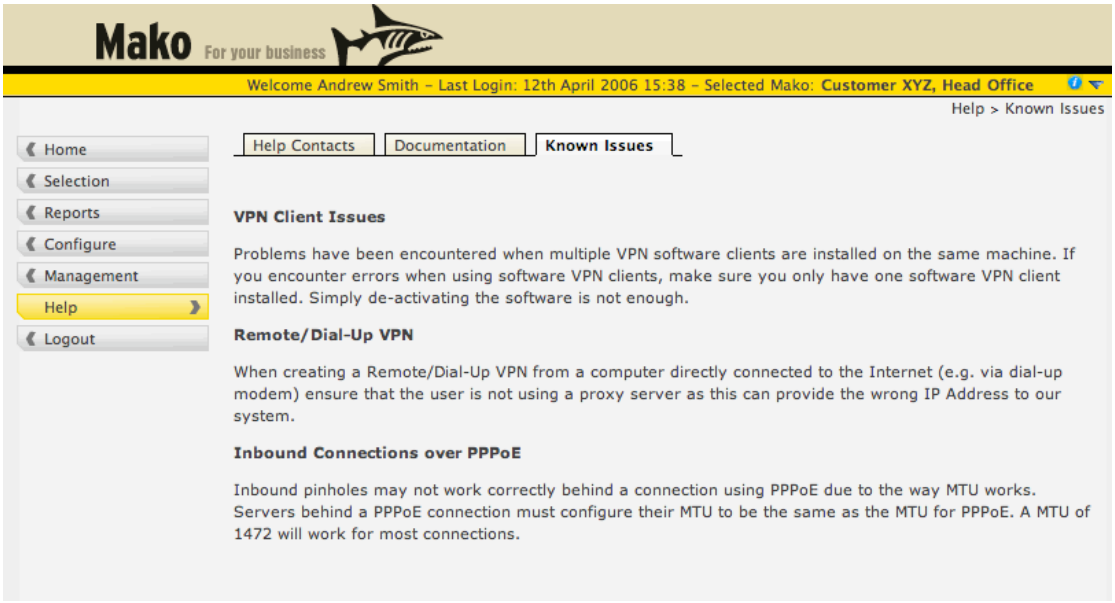
This section contains downloadable PDF documentation on nearly every aspect of the Mako System as well as product literature.



Documentation

Help: Known Issues

This area contains known issues and ways to resolve them.



Known Issues

Troubleshooting

The website provides you with detailed help on obtaining reports on your traffic, updating the configuration of your Mako, and updating your customer details.

Your Secure Customer Login:

Web Site: http://www.makonetworks.com
UserName:
Password:

What to do if:

YOU LOSE YOUR SECURE CUSTOMER PASSWORD
It is vital that you take great care of your password.

- If you lose the password you are unable to obtain help from the web site, obtain traffic reports, or update your Firewall configuration.
- If the password is exposed to a third party, your computer network immediately becomes insecure and is at risk from an attack.

You must contact your Reseller to have a new password issued to you. The Reseller is not able to provide your existing password.

Your Reseller will verify your customer identity. Because this can take some time (passwords will never be given out over the telephone) it is at least inconvenient and at worst extremely risky to lose the password.

YOU LOSE YOUR ADSL CONNECTION
You may lose your ADSL connection for a number of reasons, including telecommunications network provider problems and equipment failure.

However, you can still access the Web Site using any available Internet connection and web browser software.

The Web Site is specifically designed to work acceptably over ordinary modem connections, though of course data transfer will be slower than over your ADSL connection.

The Web Site has also been checked for compatibility against Microsoft Internet Explorer versions 4.0 and later, Netscape Navigator (Mozilla) versions 3.0 and later and several others.

Glossary of Terms

Like any specialist area, that of secure computer networking has developed a large vocabulary of jargon and technical abbreviations. Meanings do change and new terms are always being added. The list below aims to help the user to grasp the meaning of some common terms used in this document.

Please see the web site: http://whatis.techtarget.com/ for more detailed and authoritative explanations.

ADSL
Asymmetric Digital Subscriber Loop. A group of technologies used to transmit high speed (broadband) data across an analogue telephone circuit, with the channel capacity towards the subscriber being several times greater than that from the subscriber. Typical bandwidths are in megabits per second.

Browser
A software application that displays HTML formatted text and facilitates access to web sites. Examples are MS Internet Explorer, Opera and Netscape Navigator. The application provides the web browsing service, based on the HTTP protocol.

DHCP
Dynamic Host Configuration Protocol. This system allows IP addresses in a network to be assigned automatically on machine power up. The IP address may change from one network session to the next.

DMZ
A portion of a network enclosed within a Firewall System.

DNS
Domain Name Service. This service resolves host names to IP addresses.

Email
A software application for the construction and transmission of SMTP messages. Examples are MS Outlook, Eudora and Netscape Communicator.

Ethernet
Ethernet is the most widely-installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel.

Firewall System
A system which prevents unwanted Internet services from coming into or leaving the office network.

FTP
File Transfer Protocol. This is a service for bulk data transfer over the Internet.

HTML
Hyper Text Markup Language. The data structure which defines a means of formatting text, graphics, etc, on a web page for display on a Browser.

HTTP
Hyper Text Transfer Protocol. The service which transfers HTML formatted web pages to a Browser.

Hub
A device which extends the connectivity of an ethernet local area network to provide for additional computer connections.

IPsec
An industry-standard protocol for establishing secure communications at the packet level. Often used as an component in a VPN architecture.

MAC Address
Media Access Control. The hardware address of a machine's connection to a local area network. Each NIC has a unique MAC.

NIC
Network Interface Card. The component of a computer which allows connection to a local area network.

Port
The number which identifies a specific channel for communications relating to a specific Service. Ports greater than 1023 are called ephemeral ports—these are for assignment to proprietary or special purpose applications.

Router
A communications device connected between two different networks, which maps (routes) traffic between the IP addresses on each network.

Service
Services comprise three elements—a pair of communicating software applications; the definition of the data structures which the applications exchange; and the definition of the protocols by which the applications exchange data structures. Standardised services include FTP, Telnet, HTTP, SMTP, etc. There are also proprietary or special purpose services.

SMTP
Simple Mail Transfer Protocol. The service for encapsulating and sending messages to another person on the Internet, known as Email.

SSH
Secure shell. A special program providing a secure communications channel between SSH client and SSH server processes.

Switch
An ethernet connectivity device, similar to but more advanced than a Hub, which partitions traffic between connected computers to lessen congestion.

Telnet
A service which provides remote terminal login to a multi-user host.

VPN
Virtual Private Network. A method of establishing one or more secure encrypted channels between selected Internet subscribers.

Web, or World Wide Web
The client-server application which makes web sites available to Browsers.